FACHHOCHSCHULE LUDWIGSBURG
HOCHSCHULE FÜR ÖFFENTLICHE
VERWALTUNG UND FINANZEN

Wahlpflichtfach im Verwaltungszweig:

Aktuelle polizeirechtliche Probleme

Datenschutz contra Sicherheitsgesetzgebung? Entwicklungen aufgrund der Terrorismusbekämpfung

DIPLOMARBEIT

zur Erlangung des Grades einer
Diplom-Verwaltungswirtin (FH)

vorgelegt von

Hanna Oesterle
Im Wiesengrund 2
71546 Aspach

Studienjahr 2007/2008

Erstgutachter: Professor R. Buchfink
Zweitgutachter: Polizeioberrat T. Lüdecke

Inhaltsverzeichnis

Literaturverzeichnis

Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland: Ablehnung der Vorratsdatenspeicherung, DuD 2004, 603 ff

Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres: Bericht vom 31.05.2005 (A6-0174/2005), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0174+0+DOC+PDF+V0//DE, 25.01.2008 – Anlage 11

Bizer, Johann: Speicheranordnung für Verbindungsdaten, DuD 2002, 363

Büllingen, Franz: Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich, DuD 2005, 349 ff

Bull, Hans Peter: Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?, NJW 2006, 1617 ff

Bundesdruckerei: ID-Dokumente – Sicherheit ist unser Geschäft, http://www.bundesdruckerei.de/de/support/download/persoim.pdf, 20.02.2008 – Anlage 10

Bundesministerium des Innern: Bekämpfung des Terrorismus, http://www.bmi.bund.de/cln_012/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Bekaempfung__des__Terrorismus__Id__93040__de.html, 09.02.2008 – Anlage 1

Bundesministerium des Innern: Fragen und Antworten zum ePass allgemein, http://www.bmi.bund.de/cln_012/nn_1084000/Internet/Content/Themen/PaesseUndAusweise/Einzelseiten/Biometrie__FAQ.html, 01.02.2008 – Anlage 7

Bundesministerium des Innern: Gesetzgebung zur Terrorismusbekämpfung, http://www.bmi.bund.de/cln_028/nn_122754/Internet/Content/Themen/Terrorismus/DatenundFakten/Das__Terrorismusbekaempfungsergaenzungsgesetz.html, 28.01.2008 – Anlage 2

Bundesverband der Deutschen Industrie: BDI-Position zur Vorratsdatenspeicherung, DuD 2004, 606 ff

Die Datenschutzbeauftragten des Bundes und der Länder: Das Gewicht der Freiheit beim Kampf gegen den Terrorismus (Entschließung vom 26./27. Oktober 2006), http://www.bfdi.bund.de/nn_989068/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBund-Laender/72DSK-Terrorismusbek_C3_A4mpfung,templateId=raw,property=publicationFile.pdf/72DSK-Terrorismusbekämpfung.pdf, 30.01.2008 – Anlage 3

Die Datenschutzbeauftragten des Bundes und der Länder: Sondertreffen zur Terrorismusbekämpfung (Entschließung vom 01. Oktober 2001), http://www.baden-wuerttemberg.datenschutz.de/lfd/konf/2001/10_01.htm, 29.01.2008 – Anlage 6

von Denkowski, Charles: Weitere Präventivbefugnisse für das BKA?, Kriminalistik 2007, 292 ff

Dietl, Wilhelm/ Hirschmann, Kai/ Tophoven, Rolf: Das Terrorismuslexikon, Täter, Opfer, Hintergründe, 2006

Droste, Bernadette: Handbuch des Verfassungsschutzrechts, 2007

Fox, Dirk: Realisierung, Grenzen und Risiken der „Online-Durchsuchung“, DuD 2007, 827 ff

Frankfurt Airport City – Flughafen Frankfurt 2007: Fracht und Passage mit neuen Spitzenwerten, http://www.airportcity-frankfurt.de/cms/default/dok/273/273985.flughafen_frankfurt_2007_fracht_und_pass.htm, 04.02.2008 – Anlage 9

Gola, Peter/ Klug, Christoph/ Reif, Yvette: Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“, NJW 2007, 2599 ff

Golembiewski, Claudia/ Probst, Thomas: Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen, https://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf, 01.02.2008 – Anlage 8

Hansen, Markus/ Pfitzmann, Andreas: Technische Grundlagen von Online-Durchsuchung und –Beschlagnahme, DRiZ 2007, 225 ff

Hirschmann, Kai/ Gerhard, Peter (Hrsg.): Terrorismus als weltweites Phänomen, 2000

Hornung, Gerrit: Ermächtigungsgrundlage für die „Online-Durchsuchung“? Verfassungsrechtliche Anforderungen an und Grenzen für den heimlichen Zugriff auf IT-Systeme im Ermittlungsverfahren, DuD 2007, 575 ff

Huber, Bertold: Das Bankgeheimnis der Nachrichtendienste – Zur Neuregelung der Auskunftsersuchen der Nachrichtendienste durch das Terrorismusbekämpfungsergänzungsgesetz vom 9.1.2007, NJW 2007, 881 ff

Hülsmann, Werner: Gegen EU-Vorratsdatenspeicherung, DuD 2004, 734 ff

Hunsicker, Ernst: „Online-Durchsuchungen“ – Auf der Suche nach dem Machbaren, Kriminalistik 2007, 187 ff

Klewitz-Hommelsen, Sayeed: Recht auf Anonymität? Oder Anspruch auf Transparenz?, DuD 2003, 159

Koch, Cordelia: Freiheitsbeschränkung in Raten? Biometrische Merkmale und das Terrorismusbekämpfungsgesetz, HSFK-Report 5/2002, http://www.hsfk.de/downloads/rep0502.pdf, 06.02.2008 – Anlage 4

Kutscha, Martin: Verdeckte „Online-Durchsuchung“ und Unverletzlichkeit der Wohnung, NJW 2007, 1169 ff

Kutscha, Martin: Verfassungsrechtlicher Schutz des Kernbereichs privater Lebensgestaltung – nichts Neues aus Karlsruhe?, NJW 2005, 20 ff

Leutheusser-Schnarrenberger, Sabine: Vorratsdatenspeicherung – Ein vorprogrammierter Verfassungskonflikt, ZRP 2007, 9 ff

Moos, Flemming: Datenschutzrecht – Schnell erfasst, 2006

Pallasky, Ansgar: Datenschutz in Zeiten globaler Mobilität – Eine Untersuchung des Verhältnisses von Datenschutz und Gefahrenabwehr im Reisebereich, Diss., 2007

Ronellenfitsch, Michael: Datenschutzrechtliche Schranken bei der Terrorismusbekämpfung, DuD 2007, 561 ff

Roßnagel, Alexander: Verfassungspolitische und verfassungsrechtliche Fragen der Online-Durchsuchung, DRiZ 2007, 229 f

Roßnagel, Alexander/ Hornung, Gerrit: Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck, DÖV 2005, 983 ff

Roßnagel, Alexander (Hrsg.): Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003

Rublack, Susanne: Terrorismusbekämpfungsgesetz: Neue Befugnisse für die Sicherheitsbehörden, DuD 2002, 202 ff

Schaar, Peter: Das Ende der Privatsphäre - Der Weg in die Überwachungsgesellschaft, 2007

Schäuble, Wolfgang: Weltinnenpolitik im 21. Jahrhundert – Neue Herausforderungen zwischen Stabilisierung und Prävention, http://www.bmi.bund.de/cln_012/nn_165104/Internet/Content/Nachrichten/Reden/2007/11/BM__BND__Symposium.html, 15.12.2007 – Anlage 5

Schäuble, Wolfgang: Veröffentlichung des Verfassungsschutzberichts 2006, http://www.bmi.bund.de/cln_028/nn_122688/sid_3A15B626F24A7E5B3BB7D59A11A00F2E/Internet/Content/Nachrichten/Reden/2007/05/BM__VBS.html, 08.02.2008 – Anlage 12

Schneider, Werner: 22. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (Baden-Württemberg), 2001

Schulzki-Haddouti, Christiane: Im Netz der inneren Sicherheit – Die neuen Methoden der Überwachung, 2004

Ulmer, Claus D./ Schrief, Dorothee: Vorratsdatenspeicherung durch die Hintertür, DuD 2004, 591 ff

Vogelsang, Klaus: Grundrecht auf informationelle Selbstbestimmung?, 1987

Abkürzungsverzeichnis

ABl. EG	Amtsblatt der Europäischen Gemeinschaft
Abs.	Absatz
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen (Zeitschrift)
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BT-Dr	Drucksache des Bundestags
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (Entscheidungssammlung)
BVerfSchG	Bundesverfassungsschutzgesetz
CD	Compact Disc (Speichermedium)
CR	Computer und Recht (Zeitschrift)
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DRiZ	Deutsche Richterzeitung
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EG	Europäische Gemeinschaft
etc.	et cetera
EuGH	Europäischer Gerichtshof
f.	folgende
ff.	fortfolgende
GG	Grundgesetz der Bundesrepublik Deutschland
GVBl.	Gesetz- und Verordnungsblatt
Hrsg.	Herausgeber
HSFK	Hessische Stiftung Friedens- und Konfliktforschung
i.V.m.	in Verbindung mit
LDSG	Landesdatenschutzgesetz

MAD	Militärischer Abschirmdienst
MADG	Gesetz über den Militärischen Abschirmdienst
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
NRW	Nordrhein-Westfalen
S.	Seite
StPO	Strafprozessordnung
TerrBkG	Terrorismusbekämpfungsgesetz
TKG	Telekommunikationsgesetz
USB-Stick	Speichermedium
vgl.	vergleiche
z.B.	zum Beispiel
ZRP	Zeitschrift für Rechtspolitik

Anlagenverzeichnis

Anlage 1:

Bundesministerium des Innern: Bekämpfung des Terrorismus, http://www.bmi.bund.de/cln_012/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Bekaempfung__des__Terrorismus__Id__93040__de.html (09.02.2008)

Anlage 2:

Bundesministerium des Innern: Gesetzgebung zur Terrorismusbekämpfung, http://www.bmi.bund.de/cln_028/nn_122754/Internet/Content/Themen/Terrorismus/DatenundFakten/Das__Terrorismusbekaempfungsergaenzungsgesetz.html (28.01.2008)

Anlage 3:

Die Datenschutzbeauftragten des Bundes und der Länder: Das Gewicht der Freiheit beim Kampf gegen den Terrorismus (Entschließung vom 26./27. Oktober 2006), http://www.bfdi.bund.de/nn_989068/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DSBund-Laender/72DSK-Terrorismusbek_C3_A4mpfung,templateId=raw,property=publicationFile.pdf/72DSK-Terrorismusbekämpfung.pdf (30.01.2008)

Anlage 4:

Koch, Cordelia: Freiheitsbeschränkung in Raten? Biometrische Merkmale und das Terrorismusbekämpfungsgesetz, HSFK-Report 5/2002, http://www.hsfk.de/downloads/rep0502.pdf (06.02.2008)
- auszugsweise -

Anlage 5:

Bundesinnenminister Dr. Wolfgang Schäuble: Weltinnenpolitik im 21. Jahrhundert – Neue Herausforderungen zwischen Stabilisierung und Prävention, http://www.bmi.bund.de/cln_012/nn_165104/Internet/Content/Nachrichten/Reden/2007/11/BM__BND__Symposium.html (15.12.2007)
- auszugsweise -

Anlage 6:

Die Datenschutzbeauftragten des Bundes und der Länder: Sondertreffen zur Terrorismusbekämpfung (Entschließung vom 01. Oktober 2001), http://www.baden-wuerttemberg.datenschutz.de/lfd/konf/2001/10_01.htm (29.01.2008)

Anlage 7:

Bundesministerium des Innern: Fragen und Antworten zum ePass allgemein, http://www.bmi.bund.de/cln_012/nn_1084000/Internet/Content/Themen/PasseUndAusweise/Einzelseiten/Biometrie__FAQ.html (01.02.2008)

Anlage 8:

Golembiewski, Claudia/ Probst, Thomas: Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen, https://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf (01.02.2008)
- auszugsweise -

Anlage 9:

Frankfurt Airport City – Flughafen Frankfurt 2007: Fracht und Passage mit neuen Spitzenwerten, http://www.airportcity-frankfurt.de/cms/default/dok/273/273985.flughafen_frankfurt_2007_fracht_und_pass.htm (04.02.2008)
- auszugsweise -

Anlage 10:

Bundesdruckerei: ID-Dokumente – Sicherheit ist unser Geschäft, http://www.bundesdruckerei.de/de/support/download/persoim.pdf (20.02.2008)
- auszugsweise -

Anlage 11:

Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres: Bericht vom 31.05.2005 (A6-0174/2005), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2005-0174+0+DOC+PDF+V0//DE (25.01.2008)
- auszugsweise -

Anlage 12:

Bundesinnenminister Dr. Wolfgang Schäuble: Veröffentlichung des Verfassungsschutzberichts 2006, http://www.bmi.bund.de/cln_028/nn_122688/sid_3A15B626F24A7E5B3BB7D59A11A00F2E/Internet/Content/Nachrichten/Reden/2007/05/BM__VBS.html (08.02.2008)
- auszugsweise -

1 Der Datenschutz – ein umstrittenes Rechtsgebiet

Zu keiner Zeit war der Datenschutz völlig unangefochten. Es gab schon immer Vorbehalte. Denn durch den Datenschutz werden die Informationsbeschaffung und die Informationsverwendung sowohl für die Verwaltung, als auch für die Wirtschaft beschränkt und manch eine Arbeit wird umständlicher, als sie es ohne die datenschutzrechtlichen Regelungen wäre. Insbesondere um seine Pflicht zu erfüllen, das Staatsgefüge zusammenzuhalten und es besonders in Krisensituationen zu schützen, benötigt der Staat Informationen und muss mit diesen arbeiten können. Dies kollidiert allerdings von jeher mit dem Interesse des Einzelnen an seiner Privatsphäre, was auch beinhaltet, dass nicht alle ihn betreffenden Informationen ohne weiteres für jeden zugänglich sind.

Nahezu alle Gesetzesvorhaben und sonstigen Maßnahmen, die den Datenschutz stärken sollten, waren in der politischen Debatte daher heftig umstritten. Auch Dank der Autorität des Bundesverfassungsgerichtes, welches bereits in den 1980er Jahren Teile eines Gesetzes aus datenschutzrechtlichen Gründen für verfassungswidrig erklärte, konnte die Datenschutzgesetzgebung den heutigen Stand erreichen.

Trotzdem ist die Versuchung heutzutage immer noch sehr groß, in Krisensituationen die staatlichen Eingriffsbefugnisse auf Kosten des Datenschutzes zu erweitern. So kann nach außen demonstriert werden, dass man bereit ist, zu handeln.

Allerdings wurde die Daseinsberechtigung des Datenschutzes noch nie so massiv in Frage gestellt, wie nach den Terroranschlägen in den USA am 11. September 2001.[1] Diese Ereignisse setzten in Deutschland eine Gesetzeswelle in Gang, die zum Ziel hatte, die Möglichkeiten zur Bekämpfung und Verfolgung des Terrorismus zu verbessern. Die Neuregelungen haben teilweise erhebliche Einschränkungen des Datenschutzes zur Folge.

---

[1] Schneider, 8.

„Wer nichts zu verbergen hat, benötigt keinen Datenschutz!“ So lautet ein Argument, welches für diese Einschnitte herangezogen wurde und immer noch herangezogen wird. Auch wurde der Datenschutz als Täterschutz bezeichnet, denn durch die datenschutzrechtlichen Regelungen würde die Verhinderung beziehungsweise die Aufklärung von Straftaten unnötigerweise erschwert.[1] Die Änderungen bezüglich des Datenschutzes im Zuge der Antiterrormaßnahmen sind von großer Bedeutung für jeden einzelnen Bürger, da sie auch Auswirkungen auf seine persönlichen Grundrechte haben.

Daher sollen im Folgenden einige dieser, in der einschlägigen Literatur häufig diskutierten, gesetzlichen Entwicklungen in Deutschland seit dem 11. September 2001 und ihre Auswirkungen auf den Datenschutz näher beleuchtet werden. Dabei steht die Frage im Mittelpunkt, inwieweit Terrorismusbekämpfung und Datenschutz miteinander in Konflikt stehen und ob eine wirksame Terrorismusbekämpfung im Einklang mit den datenschutzrechtlichen Regelungen erfolgen kann.

2 Die rechtliche Entwicklung des Datenschutzes

Wenn heutzutage von Datenschutz gesprochen wird, so ist damit nicht etwa der Schutz von Daten gemeint. Der Datenschutz reicht viel weiter. Er soll den Einzelnen davor schützen, dass er durch den Umgang von Anderen mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird (§ 1 Abs. 1 BDSG).
Unter diesen so genannten personenbezogenen Daten sind laut § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zu verstehen. Sobald Daten einer natürlichen Person zugeordnet werden können, liegt der Personenbezug vor. Dieser liegt nicht vor, wenn es sich um

[1] Schaar, 22 f.

Sammelangaben über Personengruppen oder um anonyme Informationen handelt.[1]
Doch wie kam es zu diesen datenschutzrechtlichen Regelungen?

2.1 Die Anfänge

Die Diskussion über die Notwendigkeit des Datenschutzes in Deutschland begann Ende der 1960er Jahre. Im Hinblick auf die sich schnell entwickelnden Technologien zur automatischen Datenverarbeitung und die zunehmende Speicherung von Daten in zentralen Datenbanken wurde die Notwendigkeit gesehen, den Umgang mit Daten gesetzlich festzulegen.[2] Durch den Datenschutz sollten die Würde, die Privatsphäre und die Handlungsfreiheit des Einzelnen gewährleistet werden.[3]
Seit dem Jahr 1970 ist der Datenschutz in Deutschland gesetzlich verankert – anfangs nur im Bundesland Hessen, dann nach und nach in der ganzen Bundesrepublik. Gegenstand dieser Regelungen war zunächst der Schutz bereits erhobener Daten vor den Zugriffen von und dem Missbrauch durch Unbefugte (vgl. § 2 LDSG Hessen von 1970[4]).

2.2 Das Volkszählungsurteil

Ein sehr bedeutsamer Meilenstein in der Entwicklung des Datenschutzrechts ist das so genannte Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983.[5] Dieses Urteil prägt bis heute den rechtlichen Rahmen für den Umgang mit personenbezogenen Daten in Deutschland und erwähnt erstmals das Grundrecht auf informationelle Selbstbestimmung.[6]
Die für das Jahr 1983 geplante Volkszählung sollte den Staat und die Wissenschaft mit verlässlichen statistischen Angaben versorgen. In der

---

[1] Moos, 22.
[2] Abel in Roßnagel, 195 f.
[3] Schaar, S. 21.
[4] GVBl. I (Hessen) 1970, 625.
[5] Moos, 3.
[6] Schaar, 101.

Öffentlichkeit entwickelte sich eine heftige Diskussion darüber, zu welchen Zwecken der Staat diese Daten „wirklich“ erheben wolle und wie er mit diesen Datenmengen umgehen würde. Teilweise wurden Vermutungen laut, die erhobenen Daten würden an den Verfassungsschutz weitergeleitet, um so lückenlos alle mutmaßlichen Verfassungsfeinde erfassen zu können.[1]
Durch die Verfassungsbeschwerden, die gegen das „Volkszählungsgesetz 1983“ eingelegt wurden und aufgrund der generellen Skepsis in der Bevölkerung kam das Gericht zu der Überzeugung, dass bei den Bürgern aufgrund der modernen Datenverarbeitung eine Furcht vor unkontrollierter Persönlichkeitserfassung bestehe. Es sah deshalb die Notwendigkeit, die verfassungsrechtlichen Grundlagen des Datenschutzes umfassender zu prüfen.[2]

Nach Überzeugung des BVerfG ergibt sich aus dem allgemeinen Persönlichkeitsrecht (Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG) die Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[3]
Im Hinblick auf die Möglichkeiten der automatischen Datenverarbeitung bedürfe diese Befugnis in besonderem Maße des Schutzes. Denn es bestehe die Gefahr, dass aus den bestehenden Datensammlungen ein teilweise oder weitgehend vollständiges Persönlichkeitsbild des Einzelnen erstellt werde, welches dieser nicht auf Richtigkeit und Verwendung kontrollieren könne. Diese Möglichkeiten der fremden Einsichtnahme könnten sich durch den psychischen Druck vermeintlicher öffentlicher Anteilnahme auf das Verhalten des Einzelnen auswirken, ihn so in seiner Freiheit wesentlich hemmen und an der Ausübung seiner Grundrechte hindern. Wer nämlich nicht wisse, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben würden, würde versuchen, nicht durch solche

[1] Schaar, 99 f.
[2] BVerfG, BVerfGE 65, 4.
[3] BVerfG, BVerfGE 65, 1.

Verhaltensweisen aufzufallen und statt dessen auf die Ausübung seiner Grundrechte (z.B. Artikel 8 GG: Versammlungsfreiheit) verzichten. So würden nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigt, sondern auch das Gemeinwohl. Denn Selbstbestimmung sei eine elementare Funktionsbedingung einer Demokratie, die gerade auf die Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründet ist.[1]
Aufgrund dieser Tatsachen setze die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.[2]

Das informationelle Selbstbestimmungsrecht aus dem Volkszählungsurteil geht weit über die Regelungen des ersten und damals gültigen Bundesdatenschutzgesetzes von 1976 hinaus. Dieses BDSG schützte die personenbezogenen Daten nur vor Missbrauch bei der Speicherung, Übermittlung, Veränderung und Löschung (vgl. § 1 BDSG in der Fassung vom 27. Januar 1977[3]); es gewährte dem Einzelnen nicht die grundsätzlich uneingeschränkte Entscheidungsfreiheit über den Umgang mit seinen personenbezogenen Daten.[4]

Da alle Betroffenen jedoch in eine soziale Gemeinschaft eingebunden sind, kann auch dieses Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährt werden. Grundsätzlich müssen Einschränkungen im überwiegenden Allgemeininteresse hingenommen werden. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, aus welcher sich die Voraussetzungen und der Umfang der Beschränkung klar ergeben muss. Außerdem hat der Gesetzgeber bei seinen Regelungen den Grundsatz der Verhältnismäßigkeit zu beachten.[5] Hierbei hat auch

---

[1] BVerfG, BVerfGE 65, 42 f.
[2] BVerfG, BVerfGE 65, 43.
[3] BGBl I 1977, 201.
[4] Vogelsang, 54.
[5] BVerfG, BVerfGE 65, 43 f.

eine Interessenabwägung gegenüber anderen kollidierenden Grundrechten zu erfolgen.[1]

Die Reaktionen auf das Volkszählungsurteil waren nicht nur positiv. Kritiker wandten ein, dass der Datenschutz zur Bürokratisierung und Verrechtlichung führen könne, wenn alle Datenerhebungen und die Datenverarbeitung unter einen Genehmigungsvorbehalt gestellt würden.[2]
Es zeigt sich nun, dass diese bereits vor circa 25 Jahren aufgeworfenen Bedenken teilweise tatsächlich eingetroffen sind.
In vielen Bereichen wurde nach dem Volkszählungsurteil der Umgang mit personenbezogenen Daten geregelt. Jedoch ging es meist darum, die behördliche Praxis abzusichern und neue Verarbeitungsbefugnisse zu schaffen, anstatt den Umfang der Verarbeitung zu beschränken.[3]
Dies führte zu dem Ergebnis, dass die Zahl der gesetzlichen Datenschutzregelungen geradezu explodierte und das Datenschutzrecht daher so unübersichtlich geworden ist, dass heute eine Entbürokratisierung notwendig wäre.[4]

2.3 Die EG-Datenschutzrichtlinie

Nachdem die Anforderungen des Bundesverfassungsgerichts aus dem Volkszählungsurteil in einem mühsamen Gesetzgebungsverfahren schließlich im Jahr 1990 auch im BDSG umgesetzt worden waren, gab es im Jahr 1995 erneut einen Grund zur Überarbeitung der Datenschutzgesetze. Denn die Diskussion um den Datenschutz hatte nun auch die Europäische Gemeinschaft erreicht. Um einen Ausgleich des Datenschutzniveaus in den einzelnen Mitgliedsstaaten der Europäischen Union herbeizuführen und einen europarechtlichen Rahmen für das nationale Datenschutzrecht festzulegen, wurde am 24. Oktober 1995 die

---

[1] Bull, NJW 2006, 1617, 1622 f.
[2] Vogelsang, 34.
[3] Schaar, 103.
[4] Bull, NJW 2006, 1617.

„Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (Richtlinie 95/46/EG[1]) unterzeichnet.[2] Es werden Fragen zur Anwendbarkeit des Datenschutzrechts geklärt, sowie allgemeine Grundsätze für die Qualität und die Zulässigkeit der Verarbeitung personenbezogener Daten festgelegt. Außerdem sind spezielle Bestimmungen für die Übermittlung personenbezogener Daten in Drittländer enthalten.[3]
Seit dem 12. Juni 2002 existiert die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[4]. Sie enthält spezielle Vorschriften für den Telekommunikationssektor.
Auf den Inhalt dieser Richtlinien wird nur an den Stellen eingegangen, an denen diese zur Anwendung kommen.

2.4 Die Grundsätze des Datenschutzes

Aus diesen Entwicklungen heraus entstanden Grundsätze, die beim Umgang mit personenbezogenen Daten generell Anwendung finden. Hier wird auch das informationelle Selbstbestimmungsrecht berücksichtigt.

Entsprechend dem Grundsatz des „Datenverarbeitungsverbots mit Erlaubnisvorbehalt“ ist der Umgang mit personenbezogenen Daten nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder wenn der Betroffene einwilligt (§ 4 Abs. 1 BDSG).

Werden Daten erhoben, so sind sie grundsätzlich beim Betroffenen direkt zu erheben. Nur in gesetzlich geregelten Ausnahmefällen dürfen Daten ohne Mitwirkung des Betroffenen erhoben werden (Grundsatz der Direkterhebung, § 4 Abs. 2 BDSG).

---

[1] ABl. EG Nr. L 281, 31 ff.
[2] Abel in Roßnagel, 212 f.
[3] Moos, 13 f.
[4] ABl. EG Nr. L 201, 37 f.

Der Zweckbindungsgrundsatz besagt, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nur für diese Zwecke weiterverarbeitet werden dürfen (§ 14 Abs. 1 BDSG).[1] Diese Regelung beruht darauf, dass der Bürger ein Recht hat zu wissen, wer was wann und bei welcher Gelegenheit über ihn weiß.[2]

Gemäß dem Erforderlichkeitsgrundsatz ist der Umgang mit personenbezogenen Daten auf das für die Erreichung des jeweiligen Zwecks notwendige Maß zu beschränken. Eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten darf nur erfolgen, wenn dies zur rechtmäßigen Aufgabenerfüllung der Stelle erforderlich ist, die diese Daten verarbeitet (z.B. § 28 Abs. 1 Nr. 2 BDSG).

Außerdem gibt es noch den Grundsatz der Datenvermeidung und Datensparsamkeit. Danach soll die Grundeinstellung der Daten verarbeitenden Stellen gemäß § 3 a BDSG sein, keine oder so wenige Daten wie möglich zu erheben, zu verarbeiten und zu nutzen. Es soll das Entstehen personenbezogener Daten von vornherein möglichst vermieden werden. Dies kann zum Beispiel dadurch erfolgen, dass die Daten anonymisiert oder pseudonymisiert werden.[3]
Dieser Grundsatz darf jedoch nicht so verstanden werden, dass der Verarbeitungszweck nur dann verfolgt werden darf, wenn dabei keine personenbezogenen Daten entstehen. Sondern es muss darauf geachtet werden, diejenige Form des Umgangs zu verwenden, die am wenigsten personenbezogene Daten erfordert.[4]

---

[1] Moos, 50.
[2] BVerfG, BVerfGE 65, 43 ff.
[3] Moos, 58 ff.
[4] Bull, NJW 2006, 1619.

2.5 Die datenschutzrechtliche Situation heute

Nach fast 30 Jahren seines Bestehens ist der Datenschutz zur Selbstverständlichkeit geworden. Verwaltung und Wirtschaft haben sich an die Anforderungen des Datenschutzrechts gewöhnt und ihre Praxis weitgehend auf diese eingestellt. Laut einer Untersuchung beinhalten die Tätigkeitsberichte der Datenschutzbeauftragten aus den Jahren 1998 bis 2002 im öffentlichen Sektor kaum noch ernsthafte Defizite bei der Umsetzung des Datenschutzrechts.[1] Wird gegen die Datenschutzvorschriften verstoßen, so bleibt dies nicht folgenlos, sondern wird sanktioniert und in Zukunft vermieden.

Jedoch wird insbesondere im Zuge der Bekämpfung von organisierter Kriminalität und Terrorismus von Seiten des Gesetzgebers immer wieder versucht, die Eingriffsbefugnisse der Sicherheitsbehörden in die Privatsphäre zu erweitern, was von den Datenschützern nicht ohne Weiteres hingenommen wird.

Diese Auseinandersetzungen aufgrund unterschiedlicher Zielsetzungen von Gesetzgeber und Datenschützern werden niemals abgeschlossen sein und können auch nicht vermieden werden. Indem unterschiedliche Ansichten in der öffentlichen Diskussion dargelegt werden können, kann immer auf einen Kompromiss hingewirkt werden, der sowohl die Freiheit als auch die Sicherheit der Bürger berücksichtigt. Im Zulassen dieser öffentlichen Diskussion und in der angemessenen Reaktion darauf, bewährt sich bereits der Rechtsstaat und nicht erst in der vollständigen Einhaltung aller Verfassungs- und Gesetzesnormen.[2]

---

[1] Klewitz-Hommelsen, DuD 2003, 159.
[2] Bull, NJW 2006, 1617.

3 Die Terrorismusbekämpfung

Seit den Terroranschlägen auf das World Trade Center und das Pentagon in den USA am 11. September 2001 ist das Thema Terrorismus ständig gegenwärtig. Zwar gab es zuvor bereits terroristische Attentate, wie zum Beispiel die Anschläge der Roten Armee Fraktion in den 1970er Jahren in Deutschland oder die Anschläge auf die US-Botschaften in Nairobi und Darressalam im August 1998. Jedoch waren die des 11. Septembers 2001 in Bezug auf Ausmaß und Brutalität bis dahin beispiellos. Sie zeigten der gesamten westlichen Welt, wie verwundbar sie und ihre offene Gesellschaft ist. Denn die Anschläge können sich gegen jeden richten.
Zwar war Deutschland von diesen Geschehnissen nicht unmittelbar betroffen. Die Tatsache, dass einige der maßgebenden Attentäter vom 11. September 2001 zuvor in Deutschland gelebt hatten, zeigte jedoch, dass der Terrorismus nicht so weit entfernt ist, wie man gerne glauben mochte. Daher wurde auch hierzulande vehement nach wirksamen Mitteln zum Schutz vor Terrorismus und zur Verhinderung von Anschlägen gesucht.

3.1 Der Terrorismusbegriff

Bis heute gibt es keine einheitliche, allgemein anerkannte Definition des Terrorismusbegriffs, da die Ansichten über dessen Inhalt teilweise weit auseinander gehen.[1] Die weiteren Ausführungen folgen der Definition, dass es sich bei Terrorismus um „planmäßig vorbereitete, schockierende Gewaltanschläge gegen eine politische Ordnung aus dem Untergrund“[2] handelt. Die Anschläge sollen allgemeine Unsicherheit und Schrecken, aber auch Sympathie und Unterstützungsbereitschaft erzeugen.
Terrorismus wird bevorzugt von relativ schwachen Gruppen genutzt. Da sie nicht die Möglichkeiten haben, dem Gegner offen entgegenzutreten, erfolgen die Anschläge aus dem Untergrund.

---

[1] Dietl/Hirschmann/Tophoven, 19.
[2] Waldmann in Hirschmann/Gerhard, 11.

Um eine möglichst große öffentliche Aufmerksamkeit zu erregen, müssen die Aktionen so spektakulär und schockierend wie möglich sein. Dies ist meist dann der Fall, wenn sie sich gezielt über jeweils geltende rechtliche und moralische Konventionen hinwegsetzen und sich durch besondere Unmenschlichkeit, Willkür und Brutalität auszeichnen.[1]

Ebenso charakteristisch ist es, dass es bei einer Gewalttat nicht um die getöteten Menschen oder die zerstörten Gebäude geht. Sie hat lediglich einen symbolischen Stellenwert und ist Träger einer Botschaft. Zum einen wollen die Terroristen eine allgemeine Stimmung der Furcht und des Schreckens erzeugen, um das Vertrauen in den Staat und seine Fähigkeit, den Bürger zu schützen, zu untergraben. Zum anderen werben sie damit um Sympathie und Beistand für ihr politisches Anliegen. Man spricht daher auch von Terrorismus als Kommunikationsstrategie.[2]

Ein weiterer Aspekt des Terrorismus ist die Provokation. Terroristen wollen mit ihren Aktionen die andere Seite reizen, bis sie zum Gegenschlag ausholt. Die Staatsführung soll zu einer repressiven Überreaktion verleitet werden, die dann den angestrebten Protest im Volk auslöst. Dies kann nur dann funktionieren, wenn der Gegner auch tatsächlich mitspielt. Es besteht daher eine Reaktionsabhängigkeit der Terroristen. Meist ist es dem Gegner jedoch kaum möglich, nicht zu reagieren, da er sonst riskiert, sein Gesicht zu verlieren und als Versager zu erscheinen.[3]

Terrorismus beruht also auf drei Elementen. Das erste Element ist der Gewaltakt selber oder die Androhung eines solchen durch die Gewaltakteure. Dieser soll als zweites Element eine emotionale Reaktion bei den Opfern hervorrufen, wodurch die eigentliche Zielgruppe, um deren emotionale Beeinflussung es geht, zu einer bestimmten Verhaltensweise bewegt werden soll. Dies stellt das dritte Element dar.[4]

---

[1] Waldmann in Hirschmann/Gerhard, 11 f.
[2] Waldmann in Hirschmann/Gerhard, 13.
[3] Waldmann in Hirschmann/Gerhard, 22 f.
[4] Waldmann in Hirschmann/Gerhard, 21.

Terrorismus gibt es in mehreren unterschiedlichen Ausrichtungen. Zum einen spricht man vom ethno-nationalen Terrorismus, bei dem es um separatistische Forderungen bis hin zum eigenen Staat geht (z.B. Irisch-Republikanische Armee (IRA) in Nordirland). Zum anderen existiert ein ideologisch-weltanschaulicher Terrorismus, der wiederum in zwei Richtungen aufgegliedert ist, nämlich in den sozialrevolutionären und in den ideologisch-religiösen Terrorismus. Ziel des sozialrevolutionären Terrorismus ist es, eine ideologische und politische Neuausrichtung der Gesellschaft zu erreichen (z.B. Rote-Armee-Fraktion (RAF) in Deutschland).[1] Die Ausrichtung, die als Einzige seit den 1980er Jahren stark zugenommen hat, ist die ideologisch-religiöse. Hierbei werden bestimmte Teile der Buchreligionen (Islam, Judentum, Christentum) aus der Gesamtlehre herausgelöst, in Bezug auf die Politik interpretiert und als religiös bestimmt und vorgegeben angesehen. Die wichtigste Strömung innerhalb dieser Ausrichtung ist der islamistische Terrorismus.[2] Aus diesem Teil des Terrorismus waren auch die Anschläge vom 11. September 2001 in den USA motiviert.

Der moderne Islamismus richtet sich gegen die Regierungen im eigenen Land, da sie als tyrannisch empfunden werden. Außerdem will man sich gegen den Einfluss des „Westens“ wehren, der für wirtschaftliche und kulturelle Probleme, sowie für die politische Ohnmacht der islamischen Welt verantwortlich gemacht wird.[3] Der Islamismus ist eine politische Ideologie, die vorgibt, religiös zu sein und den Anspruch erhebt, die einzig wahre Auslegung des Glaubens darzustellen. Die gesamte Gesellschaft soll unter Allahs Herrschaft und Gesetz gebracht werden, so wie es die Schriften vorschreiben. Die Demokratie sowie der weltliche Nationalstaat werden abgelehnt, da darin der Versuch des Westens gesehen wird, die Gemeinschaft des Islam zu spalten und die Dominanz über die muslimische Welt zu erlangen.[4]

---

[1] Dietl/Hirschmann/Tophoven, 22 f.
[2] Dietl/Hirschmann/Tophoven, 24.
[3] Dietl/Hirschmann/Tophoven, 129.
[4] Dietl/Hirschmann/Tophoven, 126.

Eine besondere Herausforderung der aktuellen Situation besteht darin, dass es sich um eine abstrakte Bedrohung handelt. Es ist nicht bekannt, wer genau der Gegner ist, wo er sich aufhält, über welche Waffensysteme er verfügt und was er vorhat. Außerdem sind viele der heutigen Gegner nicht mehr abzuschrecken.[1] Denn es handelt sich dabei meist um Selbstmordattentäter, die nach der Tat religiös erhöht werden und den Status eines Märtyrers erhalten, der im Kampf gegen die „Ungläubigen" gefallen ist. So wird er zum sicheren Anwärter auf einen Platz im Paradies.[2]

Eine weitere Problematik stellt die Organisationsstruktur der Terrorgruppen dar. Heutzutage sind diese nicht mehr hierarchisch strukturiert, da die Ideologie den Rahmen vorgibt. Hieraus resultiert ein großes Bekämpfungsproblem, da es nicht genügt, die Anführer der Terroristen zu verhaften oder zu töten. Denn die Ideologie existiert trotzdem weiter.[3] Es besteht ein weltweites Netzwerk mit potentiellen Tätern, die unauffällig und sozial eingebettet in der Gesellschaft leben und man kann nicht wissen, wann und zu welchem Zweck sie „aktiviert" werden.

3.2 Die Mittel zur Bekämpfung des Terrorismus

Wie bereits dargestellt (vgl. Ziffer 3.1), ist es zu einer wirksamen Terrorismusbekämpfung nicht ausreichend, sich auf die Verfolgung einzelner herausragender Terroristen zu beschränken. Selbst wenn diese einzelnen Persönlichkeiten nicht mehr aktiv wären, hätte das nicht automatisch das Ende terroristischer Aktivitäten zur Folge.

Bei der Bekämpfung sind stattdessen weitere Aspekte zu beachten, die auch die Anti-Terror-Politik des Bundes bestimmen. So wird angestrebt, dem Terrorismus wirksam vorzubeugen. Hierzu müssen die Probleme aus den instabilen Herkunftsregionen des Terrorismus angegangen und gelöst

---

[1] Dietl/Hirschmann/Tophoven, 11.
[2] Dietl/Hirschmann/Tophoven, 249 f.
[3] Dietl/Hirschmann/Tophoven, 29 f.

werden, um so der Ideologie den Boden zu entziehen. Auch in der Bundesrepublik selbst wird versucht, dem Terrorismus energisch entgegenzutreten und Terroristen bereits an der Einreise zu hindern. Um dem transnational handelnden Netzwerk der Terroristen wirksamer begegnen zu können, ist eine gute internationale Zusammenarbeit im Hinblick auf den Informationsaustausch und die Fahndung nach Terroristen sehr wichtig. Nicht zuletzt sind Sicherheitsvorkehrungen an die Bedrohungslage anzupassen, um die Bürger zu schützen und Anschläge in Deutschland zu verhindern.[1] Dies erfolgte durch zahlreiche Änderungen der Sicherheitsgesetzgebung.

3.3 Entwicklungen in der Sicherheitsgesetzgebung seit September 2001

Die Schwierigkeiten, eine wirkungsvolle Sicherheitsgesetzgebung zur Terrorismusbekämpfung zu entwickeln, liegen vor allem in den Eigenschaften, die die „typischen“ kämpferischen, islamistischen Terroristen kennzeichnen. Er zeichnet sich durch eine hohe operativ-taktische Intelligenz aus, er arbeitet extrem professionell, ist auf dem neuesten Stand der Technik und handelt nach einem strategischen Gesamtkonzept. Außerdem ist er in seinem Gastland oft gesellschaftlich voll integriert und wird von einem starken Fanatismus getrieben.

Wie reagiert man auf ein solch gefährliches Phänomen am sinnvollsten?

Der Gesetzgeber leitete eine Reihe von Maßnahmen ein, um die gesetzlichen Instrumente zur Gewährleistung der Sicherheit der Bundesrepublik fortzuentwickeln.[2]

In diesem Zusammenhang wurde gefordert, „den Datenschutz tiefer zu hängen“, damit die angebliche „Hürde“ Datenschutz für eine effiziente Antiterrorgesetzgebung aus dem Weg geschafft oder zumindest

---

[1] Bundesministerium des Innern, siehe Anlage 1, 1 ff.
[2] Dietl/Hirschmann/Tophoven, 307 f.

herabgesetzt werden könnte.[1] Die bedeutendsten gesetzlichen Regelungen in diesem Zusammenhang werden im Folgenden skizziert.

3.3.1 Das Sicherheitspaket I

Am 09. November 2001 beschloss der Bundestag das erste Sicherheitspaket, welches zwei wesentliche Gesetzesänderungen enthält. Zum einen wurde das Religionsprivileg im Vereinsgesetz abgeschafft.[2] Dies hat zur Folge, dass auch religiöse Vereine verboten werden können, wenn sich ihre Tätigkeiten gegen die verfassungsmäßige Ordnung oder den Gedanken der Völkerverständigung richten oder wenn sie gegen die Strafgesetze verstoßen. Bis dahin waren religiöse Vereine weitgehend von der Möglichkeit eines Verbots ausgenommen. Erste „Leidtragende“ war die islamisch extremistische Vereinigung Kalifatstaat unter ihrem Führer Metin Kaplan, die der damalige Bundesinnenminister Otto Schily am 12. Dezember 2001 verbot, da sie unter anderem gegen die demokratische Grundordnung Deutschlands gehetzt hatte.
Zum anderen wurde im Strafgesetzbuch der § 129 b eingeführt[3], der es möglich macht, die Mitgliedschaft und Unterstützung terroristischer Gruppierungen auch dann zu verfolgen, wenn diese nicht in Deutschland ansässig sind. So soll verhindert werden, dass sich die Bundesrepublik zu einem Rückzugsraum für internationale Terroristen entwickelt.[4]

3.3.2 Das Sicherheitspaket II

Noch im Dezember 2001 wurde das „Gesetz zur Bekämpfung des internationalen Terrorismus“ (Terrorismusbekämpfungsgesetz[5]) verabschiedet und trat im Januar 2002 in Kraft. Bei diesem Gesetz handelt es sich um ein Artikelgesetz. Das bedeutet, dass kein neues Gesetz geschaffen, sondern Änderungen an bereits bestehenden Gesetzen

---

[1] Schaar, 127.
[2] BGBl. I 2001, 3319.
[3] BGBl. I 2002, 3390.
[4] Dietl/Hirschmann/Tophoven, 308.
[5] BGBl. I 2002, 361 ff.

vorgenommen wurden. Durch dieses Gesetzespaket wurde eine große Anzahl von Sicherheitsgesetzen geändert, was mit der weltweit neuen Dimension der terroristischen Bedrohung begründet wurde.[1]

Da dem Verfassungsschutz bei der Terrorismusbekämpfung eine wichtige Aufgabe zukommt, wurden dem Bundesamt für Verfassungsschutz neue Befugnisse zugeteilt (Artikel 1 TerrBkG). Diese und die Neuregelungen, die die anderen Sicherheitsbehörden (Artikel 2 und 3 TerrBkG) betreffen, werden unter Punkt 4.1 näher dargestellt. Diese Neuregelungen wurden auf fünf Jahre befristet. Vor Ablauf dieser Frist sollte eine Evaluation erfolgen, um die Wirksamkeit und die Umsetzung zu überprüfen und über das weitere Vorgehen zu entscheiden.

Die Sicherheit an Bord von deutschen Luftfahrzeugen konnte durch den Einsatz von Flugsicherheitsbegleitern des Bundesgrenzschutzes weiter erhöht werden (Artikel 6 Nr. 2 TerrBkG). Sie sollen der Entführung von Luftfahrzeugen, terroristischen Anschlägen und Geiselnahmen durch gezielte Einsätze vorbeugen.

Die Bundespolizei wurde ermächtigt, Personen innerhalb ihres Zuständigkeitsbereichs nicht nur anzuhalten und zu befragen, sondern auch mitgeführte Ausweispapiere zu überprüfen (Artikel 6 Nr. 3 TerrBkG).

In das Aufenthaltsrecht wurden Bestimmungen aufgenommen, die verhindern, dass Personen eine Aufenthaltsgenehmigung bekommen, die die freiheitliche demokratische Grundordnung oder die Sicherheit der Bundesrepublik Deutschland gefährden. Einreise und Aufenthalt ist ihnen untersagt. Außerdem wurden Grundlagen geschaffen, durch die die Zusammenarbeit der Auslandsvertretungen mit den Sicherheitsbehörden intensiviert werden kann (Artikel 11 TerrBkG).

---

[1] BT-Dr 14/7386, 35.

Durch die Änderungen im Asylverfahrensgesetz wurde die gesetzliche Grundlage für eine Sprachanalyse geschaffen, mit der die Herkunftsregion bestimmt werden kann. Fingerabdrücke und sonstige identitätssichernde Unterlagen dürfen 10 Jahre ab Unanfechtbarkeit der Asylentscheidung aufbewahrt werden. Auch können Fingerabdrücke von Asylbewerbern seit der Gesetzesänderung automatisch mit dem polizeilichen Tatortspurenbestand des Bundeskriminalamts abgeglichen werden (Artikel 12 TerrBkG).
Der Zugriff für Polizeibehörden auf das Ausländerzentralregister wurde verbessert, sodass diese im Rahmen einer Personenkontrolle oder Ähnlichem sofort feststellen können, ob sich ein Ausländer legal in Deutschland aufhält. Die Daten sind für die berechtigten Behörden nun auch online abzurufen (Artikel 13 TerrBkG).

Um zu verhindern, dass Personen sich mit fremden Ausweispapieren ausweisen, wurden Grundlagen zur Aufnahme biometrischer Merkmale in die Ausweisdokumente geschaffen (Artikel 7 und 9 TerrBkG).

Die Vereinsverbotsgründe für Ausländervereine und ausländische Vereine wurden neu gefasst und zum Teil ausgeweitet, um zu verhindern, dass gewalttätige und terroristische Organisationen von Ausländervereinen in Deutschland unterstützt werden (Artikel 9 TerrBkG).[1]

Kritiker des Gesetzes sind der Ansicht, dass die dort enthaltenen Regelungen vielfach wenig mit dem Phänomen Terrorismus zu tun haben, sondern lang gehegte Wünsche hinsichtlich erweiterter Eingriffsbefugnisse erfüllen, die weit über das Ziel einer gezielten Terrorismusbekämpfung hinausgehen.[2] Hier wird zum Beispiel die Aufnahme von biometrischen

[1] Bundesministerium des Innern, siehe Anlage 2, 2 ff.
[2] Rublack, DuD 2002, 202, 206.

Daten in Ausweispapiere[1] genannt oder die erweiterte Ermittlungsbefugnis des Bundeskriminalamts[2].

3.3.3 Das Zuwanderungsgesetz

Das am 01. Januar 2005 in Kraft getretene Gesetz enthält verschärfte Sicherheitsbestimmungen beim Aufenthaltsrecht. Danach können Personen, von denen eine terroristische Gefahr ausgeht, auf Anordnung der obersten Landesbehörden oder des Bundesinnenministeriums schneller abgeschoben werden. Falls der Abschiebung Hinderungsgründe, wie zum Beispiel Folter oder Todesstrafe im Heimatland, entgegenstehen, können verschärfte Aufenthaltsauflagen erlassen werden.[3]

3.3.4 Das Luftsicherheitsgesetz

Am 15. Januar 2005 trat das Luftsicherheitsgesetz[4] in Kraft. Dieses Gesetz dient dem Schutz vor Angriffen auf die Sicherheit des Luftverkehrs, insbesondere vor Flugzeugentführungen, Sabotageakten und terroristischen Anschlägen (§ 1 Luftsicherheitsgesetz). Die wohl bekannteste Regelung ist § 14 Abs. 3 Luftsicherheitsgesetz. Er enthält die Ermächtigung der Streitkräfte, ein Flugzeug abzuschießen, wenn nach den Umständen davon auszugehen ist, dass es als Tatwaffe gegen das Leben von Menschen eingesetzt werden soll und wenn es das einzige Mittel zur Abwehr einer gegenwärtigen Gefahr ist. In seinem Urteil vom 15. Februar 2006 entschied jedoch das BVerfG, dass § 14 Abs. 3 Luftsicherheitsgesetz nicht mit dem Grundgesetz vereinbar und daher nichtig sei.[5]

---

[1] Schneider, 18.
[2] Rublack, DuD 2002, 202, 205.
[3] Dietl/Hirschmann/Tophoven, 310 f.
[4] BGBl. I 2005, 78 ff.
[5] BVerfG, BVerfGE 115, 118 ff.

3.3.5 Das Gemeinsame-Dateien-Gesetz

Am 31. Dezember 2006 ist das „Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz)“ in Kraft getreten. Durch diese gemeinsamen Dateien soll die Zusammenarbeit der Sicherheitsbehörden gezielt unterstützt und der Informationsaustausch verbessert werden.

Eine solche gemeinsame Datei stellt die Anti-Terror-Datei dar. Terrorismusrelevante Informationen sind von den Polizeibehörden und Nachrichtendiensten des Bundes und der Länder dort einzustellen und so grundsätzlich allen Sicherheitsbehörden zugänglich zu machen.[1]

Außerdem kann das Bundesamt für Verfassungsschutz gemeinsame Dateien für eine befristete projektbezogene Zusammenarbeit mit den Nachrichtendiensten und den Polizeibehörden des Bundes und der Länder einrichten.[2]

Kritiker äußern, dass durch diese Regelungen das Trennungsgebot von Polizei und Nachrichtendienst aufgeweicht würde.[3] Dieses war nach dem zweiten Weltkrieg eingeführt worden, um zu verhindern, dass sich eine Willkürherrschaft mit Hilfe einer über nachrichtendienstliche Mittel verfügende Staatspolizei entwickeln kann.[4]

3.3.6 Das Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes

Nachdem die in Artikel 22 Abs. 2 und 3 Terrorismusbekämpfungsgesetz vorgeschriebene Evaluation der Neuregelungen erfolgt war, wurden die daraus gewonnenen Erkenntnisse im so genannten „Terrorismusbekämpfungsergänzungsgesetz“[5] umgesetzt. Es trat am 11. Januar 2007 in Kraft.

---

[1] Droste, 26.
[2] Droste, 27.
[3] Schaar, 151 ff.
[4] Droste, 13 f.
[5] BGBl. I 2007, 2 ff.

Die Anwendung der befristeten Regelungen wurde als erfolgreich und verantwortungsvoll angesehen. Deshalb wurden sie zum größten Teil unverändert beibehalten, gelten allerdings wieder nur befristet für fünf Jahre. Lediglich die Verfahrensabläufe für die Auskunftsrechte der Nachrichtendienste wurden praxisgerechter gestaltet und die Voraussetzungen für die Auskunft über Verbindungs- und Nutzungsdaten wurden praxisnäher definiert. Außerdem kann das Bundesamt für Verfassungsschutz nun seine bestehenden Auskunftsbefugnisse auch zur Aufklärung bisher noch nicht erfasster verfassungsfeindlicher Bestrebungen einsetzen, sofern diese die Bereitschaft zur Anwendung von Gewalt fördern. Zusätzlich können die Nachrichtendienste in Zukunft Fahrzeug- und Halterdaten auch automatisiert aus dem entsprechenden Register abrufen.

Bei der vorgeschriebenen Prüfung, ob die Regelungen noch gebraucht würden, wurde also festgestellt, dass man sie sogar noch erweitern muss. Dieses Vorgehen lässt befürchten, dass jede Überprüfung eine weitere Verschärfung der Regelungen und damit eine erneute Beschränkung des Datenschutzes mit sich bringen könnte.
Datenschützer äußern, dass die Befugnisse, die ursprünglich zur Terrorismusbekämpfung geschaffen wurden, immer weiter ausgedehnt und sich nicht mehr nur auf Terrorismusverdächtige beschränken würden. Zudem führe mehr Überwachung nicht automatisch zu mehr Sicherheit, sondern nur zu weniger Freiheit.[1]

[1] Die Datenschutzbeauftragten des Bundes und der Länder, siehe Anlage 3, 1.

4 Das Spannungsverhältnis zwischen Gefahrenabwehr und Datenschutz

Nicht erst seit den Terroranschlägen vom 11. September 2001 befinden sich Datenschutz und Gefahrenabwehr in einem Spannungsverhältnis. Da aber das Bedürfnis nach Sicherheit aufgrund der Bedrohung durch weitere Anschläge seitdem größer geworden ist, wird diesem Thema automatisch mehr Aufmerksamkeit zuteil.

Dieses Spannungsverhältnis ist kennzeichnend für einen demokratischen Verfassungsstaat. Die Kernthemen Freiheit und Sicherheit sind untrennbar mit dieser Organisation eines politischen Gemeinwesens verbunden. Es darf nicht nur eines von beiden verwirklicht werden, da dies entweder den totalitären Staat oder die Willkür unter den Staatsbürgern zur Folge hätte. Grundvoraussetzung und Lebensgrundlage für die Demokratie, die auf Selbstbestimmung der Bürger aufgebaut ist, sind sowohl die Freiheit, als auch die Sicherheit. Diese Selbstbestimmung kann jedoch nur in einem von Gewalt und Willkür freien Umfeld ausgeübt werden.

Notgedrungen tangiert und beschränkt jede Sicherheitsmaßnahme zur Gefahrenabwehr die Freiheit der Bürger, so wie andererseits maximale Freiheit zu Einbußen auf dem Gebiet der Sicherheit führen würde.

Sicherheit umfasst jedoch nicht nur das Recht auf Leben, sondern auch die Gewissheit, dass zum Beispiel Verträge erfüllt, erlittene Schäden ausgeglichen und Straßenverkehrsregeln befolgt werden. Dieser umfassende Sicherheitsbegriff kann daher nicht nur als Freiheitsbeschränkung verstanden werden. Sicherheit ist auch Voraussetzung für Freiheit. Mit diesem Gedanken können Sicherheitsmaßnahmen begründet werden, auch die Maßnahmen zur Terrorismusbekämpfung zum Schutz der Bürger. Der nächste Schritt muss jedoch sein, die Maßnahmen daraufhin zu überprüfen, ob sie sich in ihrer Ausgestaltung rechtfertigen lassen. Hier muss der Sicherheitserfolg dem Grad der Freiheitsbeschränkung gegenübergestellt werden.

Freiheit und Sicherheit stehen also in einem unauflösbaren Widerspruch zueinander, welcher jedoch für eine Demokratie sehr wichtig ist und der immer in einer ausgewogenen Balance gehalten werden muss.[1]

Das Verhältnis von Freiheit und Sicherheit ist nicht unveränderlich. Eine Bedrohung des Staates, wie durch Terroranschläge, kann das Verhältnis zugunsten der Sicherheit verschieben und Eingriffe in die Freiheitsbelange der Bürger rechtfertigen, die unter „normalen“ Umständen nicht akzeptabel wären. Die Maßnahmen des Gesetzgebers nach dem 11. September 2001 sind daher der Versuch, eine Ausgewogenheit zwischen Sicherheit und Freiheit herzustellen. Bei manchen Maßnahmen äußern Kritiker jedoch, dass die situationsbedingte Anpassung der Gesetze an die veränderte Sicherheitslage weit über das Ziel hinaus gehe und nicht die ausbalancierte Lösung des Sicherheitsproblems darstelle. Denn Unberechenbarkeit und Unvorhersehbarkeit ist für den Terrorismus charakteristisch, sodass Sicherheitsmaßnahmen zur Verhinderung des Terrorismus sehr weitgehend sein müssen, um einen Erfolg erzielen zu können. Die Folge davon sind erhebliche Auswirkungen auf die Freiheitsrechte der Bürger, unter anderem auch auf das informationelle Selbstbestimmungsrecht. Ob dann noch eine Balance zwischen Freiheit und Sicherheit besteht, ist fraglich.[2]

Im Folgenden sollen ausgewählte Beispiele die Veränderungen im Zusammenhang mit der Terrorismusbekämpfung und ihre Auswirkungen auf den Datenschutz darstellen.

---

[1] Koch, siehe Anlage 4, 3 f.
[2] Koch, siehe Anlage 4, 4 f.

4.1 Neue Befugnisse für die Sicherheitsbehörden

Das wichtigste Instrument im Kampf gegen den Terrorismus sei die Information und „deswegen müssen wir mehr wissen“, äußerte Bundesinnenminister Dr. Wolfgang Schäuble am 01. November 2007 in Berlin.[1]
Für die Beschaffung von wichtigen Informationen für die Sicherheit, sind in Deutschland insbesondere die Verfassungsschutzbehörden des Bundes und der Länder, der Bundesnachrichtendienst, der Militärische Abschirmdienst und zum Teil auch das Bundeskriminalamt zuständig.

4.1.1 Aufgabenbereiche

Grundsätzlich hat das Bundesamt für Verfassungsschutz in Zusammenarbeit mit den Verfassungsschutzbehörden der Länder die Aufgabe, Informationen mit Bezug zum Inland zu beschaffen und auszuwerten, die aufgrund ihrer Gefährdung der verfassungsmäßigen Ordnung für den Bestand des Staates von Wichtigkeit sind. Auch eine Tätigkeit im Ausland kann notwendig und zulässig sein.[2]

Die Aufgabe des Bundesnachrichtendienstes besteht in der Beschaffung und Auswertung von Informationen über das Ausland, welche für Deutschland von außen- und sicherheitspolitischem Interesse sind und die von anderen Staaten geheim gehalten werden. Im Gegensatz zu den Verfassungsschutzbehörden, ist der BND ein Auslandsnachrichtendienst, was jedoch nicht bedeutet, dass er nicht auch im Inland tätig werden darf.[3]

Der Militärische Abschirmdienst nimmt Verfassungsschutzaufgaben im Bereich der Bundeswehr wahr. Er sammelt Informationen über verfassungsfeindliche Bestrebungen oder sicherheitsgefährdende und

---

[1] Schäuble, siehe Anlage 5, 1.
[2] Droste, 29.
[3] Droste, 28 f.

geheimdienstliche Tätigkeiten und wertet sie aus, sofern sie sich gegen die Bundeswehr richten oder von Bundeswehrangehörigen ausgehen.[1]

Das Bundeskriminalamt ist neben dem Auslandsverkehr auch zuständig für die überörtliche Verbrechensbekämpfung im Inland. Zur Erfüllung dieser zentralen Aufgaben liefern die Länder Daten und Informationen an das BKA. Die Befugnis zur Strafverfolgung besteht nur begrenzt. Eine wichtige Funktion des BKA ist die einer Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen. Sie unterstützt die Polizei des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder sonst erheblicher Bedeutung. Dabei ist sie für den Austausch, nicht für die Erhebung der relevanten Informationen zuständig.[2]

4.1.2 Neuregelungen

Durch das Terrorismusbekämpfungsgesetz aus dem Jahr 2002[3] wurde der Beobachtungsauftrag des Bundesamtes für Verfassungsschutz im Inland (Artikel 1 Nr. 1 TerrBkG) und des Militärischen Abschirmdienstes (Artikel 2 Nr. 1 TerrBkG) erweitert auf Bestrebungen, die sich gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker, richten.
Bereits vor diesen Neuregelungen durften gewaltbereite Extremisten beobachtet werden. Nun ist auch das Vorfeld von extremistischen Bestrebungen, welches den Nährboden für Terrorismus bilden kann[4], eingeschlossen. Es geht also nicht mehr nur um geplante oder durchgeführte Gewaltanwendungen, sondern um extremistische Auffassungen.[5]

---

[1] Droste, 30.
[2] von Denkowski, Kriminalistik 2007, 292.
[3] BGBl. I 2002, 361 ff.
[4] BT-Dr 14/7386, 38.
[5] Ronellenfitsch, DuD 2007, 561, 566.

Außerdem wurden dem Bundesamt für Verfassungsschutz umfassende Auskunftsbefugnisse eingeräumt (Artikel 1 Nr. 3 TerrBkG). Bei Banken können Auskünfte über Konten und Konteninhaber eingeholt werden. Von Postdienstleistern können Informationen zu Namen, Anschriften, Postfächern und ähnlichem erfragt werden. Luftfahrtunternehmen sind verpflichtet, dem Bundesamt unter anderem Auskünfte zu Namen, Anschriften und zur Inanspruchnahme von Transportdienstleistungen zu erteilen. Auch ist es möglich, von Telekommunikations- und Teledienstleistern Informationen über Verbindungsdaten und Ähnlichem einzuholen.
Auch dem MAD und dem BND wurden entsprechende telekommunikations- und teledienstbezogene Auskunftsbefugnisse eingeräumt. Zusätzlich hat der BND Auskunftsrechte gegenüber Banken und Finanzunternehmen erhalten (Artikel 2 Nr. 4 TerrBkG, Artikel 3 Nr. 1 und 2 TerrBkG).

Mit Artikel 1 Nr. 4 TerrBkG wurde die Befugnis des Bundesamtes für Verfassungsschutz eingeführt, dass Personen, die bei einem Einsatz in Wohnungen tätig sind, zur Eigensicherung verdeckte technische Mittel einsetzen dürfen („bemannte Wanze“). Die so erlauschten Informationen dürfen verwendet werden, sofern die Maßnahme insgesamt rechtmäßig war.

Darüber hinaus darf das Bundesamt nach Artikel 1 Nr. 4 c TerrBkG unter den dort genannten Voraussetzungen technische Mittel zur Ermittlung des Standorts eines aktiv geschalteten Mobilfunkgerätes und zur Ermittlung der Geräte- und Kartennummern einsetzen („IMSI-Catcher“).

Die den Sicherheitsbehörden eingeräumten Auskunftsbefugnisse betreffen zwar meist formale Daten, jedoch sind diese durchaus geeignet, ein Bewegungsprofil über die betroffene Person zu erstellen und Erkenntnisse über Kontakte zu bestimmten Kreisen zu gewinnen. Bei stärkerem

Datenanfall kann ein zumindest hinreichend konkretes Persönlichkeitsbild sichtbar werden. Dies stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Aus diesem Grund wurde eine Kontrollmöglichkeit dieser Befugnisse geschaffen. Die so genannte G 10-Kommission (unabhängiges, an keine Weisungen gebundenes Kontrollgremium) hat vor Vollzug einer solchen Maßnahme über deren Zulässigkeit und Notwendigkeit zu befinden. Außerdem muss den Betroffenen nach Beendigung der Maßnahme Mitteilung gemacht werden, sofern der Zweck der Maßnahme dadurch nicht gefährdet wird.[1]

Das BKA besitzt seit 2002 die Befugnis, unabhängig von bereits vorliegenden Sachverhalten bei den Länderpolizeien Informationen durch Datenerhebungen bei öffentlichen und nicht-öffentlichen Stellen zu beschaffen (§ 7 Abs. 2 BKAG). So kann das BKA entgegen seiner eigentlichen Zentralstellenfunktion selbständig präventive Ermittlungen durchführen.[2]

Nach erfolgter Überprüfung der Neuregelungen von 2002 wurden die Befugnisse des Bundesamts für Verfassungsschutz, des BND sowie des MAD, soweit dessen Aufgabenkreis berührt wird, durch das Terrorismusbekämpfungsergänzungsgesetz aus dem Jahr 2007 angeglichen.
Eine zentrale Änderung gegenüber den bisherigen Regelungen ist der Wegfall der externen Kontrolle. Die Kompetenz der G 10-Kommission, sämtliche Auskunftsersuchen zu überprüfen, besteht nicht mehr. Lediglich Eingriffe in das Brief-, Post- und Fernmeldegeheimnis sind noch zu prüfen. Außer der behördeninternen Dienstaufsicht ist keine Kontrolle mehr vorhanden. Dies vermag auch die Vorschrift, dass das Parlamentarische Kontrollgremium im Abstand von sechs Monaten über die durchgeführten

---

[1] Huber, NJW 2007, 881, 881 f.
[2] von Denkowski, Kriminalistik 2007, 292, 293.

Maßnahmen nachträglich zu unterrichten ist (§ 8 a Abs. 6 BVerfSchG), nicht zu verbessern.

Zudem wurden durch die Neuregelungen das Trennungsgebot zwischen Verfassungsschutz und Polizei aufgeweicht, weshalb es zu doppelten Datenbeständen kommen kann. Dies kollidiert eindeutig mit dem datenschutzrechtlichen Grundsatz der Datensparsamkeit.[1]

Indem das BKA als eigentliche Zentralstelle selbständig Ermittlungen durchführen kann, besteht auch hier die Gefahr der Doppelerhebung von Daten. Dies wird in der Praxis mit einem Datenabgleich kontrolliert. Dadurch werden jedoch dem BKA und den Landespolizeistellen Zugriffe auf Daten ermöglicht, die nicht in ihrem Aufgabenbereich liegen. Das verstößt gegen den datenschutzrechtlichen Grundsatz der Zweckbindung.[2]

4.1.3 Wertung

Durch den erweiterten Beobachtungsauftrag des Verfassungsschutzes und des MAD ist die Entstehung einer ausufernden Datensammlung zu befürchten, die sich nicht mehr nur auf geheimdienstliche Aufklärung von eindeutig gewaltorientiertem islamischem Extremismus beschränkt.[3] Dies ist mit dem datenschutzrechtlichen Grundsatz der Datensparsamkeit nicht zu vereinbaren.

Durch den Einsatz der so genannten IMSI-Catcher besteht das Risiko, dass auch die Daten des Gesprächspartners abgefangen werden und außerdem der Inhalt der Gespräche zugänglich gemacht wird. Auch die Daten anderer in der Nähe befindlicher Mobilfunkgeräte können erfasst werden. Jeder, der über sein Mobilfunkgerät erreichbar sein will, muss

---

[1] Ronellenfitsch, DuD 2007, 561, 566.
[2] Ronellenfitsch, DuD 2007, 561, 566 f.
[3] Rublack, DuD 2002, 202, 203.

also damit rechnen, dass sein Aufenthaltsort jederzeit ermittelt werden kann. Es ist daher fraglich, ob dieser Eingriff in die informationelle Selbstbestimmung verhältnismäßig ist.[1]

Die erweiterten Befugnisse der Sicherheitsbehörden sind gerade deshalb so bedeutend, da die Eingriffe im Verborgenen stattfinden und der Betroffene davon nichts bemerkt. Im Hinblick auf den Schutz des informationellen Selbstbestimmungsrechts ist zumindest darauf zu achten, dass er nach der Maßnahme informiert wird.

Die Datenschutzbeauftragten des Bundes und der Länder warnten bereits im Oktober 2001 vor pauschalen Forderungen nach Einschränkungen des Grundrechts auf informationelle Selbstbestimmung, um dem Terrorismus besser begegnen zu können. Ihrer Ansicht nach verfügten die Sicherheits- und Strafverfolgungsbehörden zu dem Zeitpunkt bereits über weit reichende Befugnisse zur Datenverarbeitung. Man müsse eher bestehende Vollzugsdefizite abstellen, bevor man weiter in Grundrechte der Bürger eingreife. So seien bei der künftigen Gesetzgebung unbedingt die grundlegenden Rechtsstaatsprinzipien zu beachten, wie zum Beispiel das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten. Denn diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, der im Kampf gegen den Terrorismus verteidigt werden muss.[2]

---

[1] Ronellenfitsch, DuD 2007, 561, 569.
[2] Die Datenschutzbeauftragten des Bundes und der Länder, siehe Anlage 6, 1.

4.2 Biometrische Merkmale in Reisepässen

Ebenfalls im Zusammenhang mit der Debatte zur Terrorismusbekämpfung nach dem 11. September 2001 rückte die Biometrie in den Blickpunkt des öffentlichen Interesses. Mit dem Ziel, bereits die Einreise von Terroristen nach Deutschland zu verhindern, wurden gesetzliche Grundlagen für die Aufnahme von biometrischen Merkmalen in die Reisepässe geschaffen (Artikel 7 und 8 des Terrorismusbekämpfungsgesetzes[1] aus dem Jahr 2002). Danach ist es nun erlaubt, neben einem Lichtbild und der Unterschrift weitere biometrische Merkmale von Gesicht, Fingern oder Händen in Ausweispapiere aufzunehmen.

Mit Hilfe der Biometrie soll die Verifikation des Ausweisinhabers verbessert und die Identitätsprüfung automatisiert werden. Die genaue Umsetzung dieser Regelungen sollte durch ein Bundesgesetz erfolgen. Ein solches Gesetz wurde jedoch bis zum Jahr 2005 nicht erlassen.[2]

Nicht zuletzt auf Drängen der USA, die für das Fortbestehen des „Visumfreien Einreisens“ zur Bedingung machten, dass die entsprechenden Länder bis Oktober 2005 in der Lage sein mussten, Pässe mit digitalen Fotos auszustellen, wurden in der Europäischen Union diesbezüglich Regelungen getroffen. Am 18. Januar 2005 trat die EG-Verordnung „über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“[3] in Kraft. Sie gilt in Deutschland gemäß Artikel 249 des EG-Vertrags unmittelbar, sodass entgegenstehende nationale Rechtsnormen nicht mehr wirksam sind.[4]

In Deutschland wurde der elektronische Reisepass (ePass) im November 2005 eingeführt. In der Passdecke befindet sich ein Chip, auf dem neben personen- und dokumentenbezogenen Daten wie zum Beispiel Vor- und Nachname, Geburtsdatum und Gültigkeitsdauer des Passes auch

---

[1] BGBl. I 2002, 361, 366.
[2] Roßnagel/Hornung, DÖV 2005, 983.
[3] ABl. EG Nr. L 385, 1 ff.
[4] Roßnagel/Hornung, DÖV 2005, 983, 987.

biometrische Daten gespeichert werden. Bei Antragsdatum bis zum 31. Oktober 2007 wurde zunächst nur ein Passfoto gespeichert, bei Antragsdatum ab dem 01. November 2007 zusätzlich zwei Fingerabdrücke.[1] Diese zeitlich versetzte Einführung ist laut Artikel 6 der EG-Verordnung möglich.

Brisanz erlangt die Erfassung biometrischer Merkmale im Reisepass dadurch, dass diese geeignet ist, eine Grundregel unseres Rechtsstaates, nämlich die Unschuldsvermutung, umzukehren. Dazu könnte es kommen, wenn der Passinhaber entgegen der Schuldvermutung des biometrischen Systems seine Unschuld beweisen muss. Dies wäre dann der Fall, wenn er vom System nicht identifiziert werden kann und er daher beweisen muss, dass er „er selbst" ist.

Daher muss sorgsam überprüft werden, ob die Aufnahme biometrischer Merkmale in den Pass das beabsichtigte Sicherheitsziel erreicht. Zusätzlich ist zu beachten, ob diese Maßnahme in Bezug auf die dadurch eintretende Freiheitsbeschränkung verhältnismäßig ist.[2]

4.2.1 Grobe Begriffsklärung

Der Begriff „Biometrie" stammt aus dem Griechischen und beinhaltet die beiden griechischen Worte „bios" (= Leben) und „metrein" (= messen). Im vorliegenden Fall meint Biometrie eine automatische Vermessung des menschlichen Körpers, um eine automatisierte (Wieder-)Erkennung dieses Menschen zu ermöglichen.[3]

Biometrische Verfahren erfassen individuelle Eigenschaften wie zum Beispiel den Fingerabdruck, die Iris oder die Stimme und werten diese aus. Damit soll die Identifikation von Personen verbessert werden. Bei der biometrischen Erkennung werden die aktuell aufgenommenen Werte mit gespeicherten Daten verglichen. Bei der Gesichtserkennung wird zum

---

[1] Bundesministerium des Innern, siehe Anlage 7, 1.
[2] Koch, siehe Anlage 4, 2.
[3] Golembiewski/Probst, siehe Anlage 8, 1.

Beispiel eine aktuell gemachte Digitalaufnahme mit einem hinterlegten Passfoto verglichen.

Allerdings gibt es auch bei diesem Verfahren keine völlige Sicherheit. Denn es werden immer nur Ähnlichkeiten und bestimmte Grade der Übereinstimmung festgestellt. Liegen diese Übereinstimmungen über einem festgelegten Schwellenwert, so gilt die Identität als gesichert. Dieser Schwellenwert ist von erheblicher Bedeutung. Wird er nämlich zu hoch gewählt, werden möglicherweise bei Zugangskontrollen Berechtigte nicht erkannt. Wird der Schwellenwert zu niedrig gewählt, werden auch Unberechtigte durchgelassen. Denn durch Messfehler, durch Veränderung der körperlichen Merkmale durch Verletzung oder Krankheit oder durch schlechte Qualität der Daten kann die Erkennungsleistung beeinträchtigt werden.[1]

Es gibt mit der Verifikation und der Identifikation zwei Arten von biometrischer Erkennung. Die Verifikation bestätigt oder widerlegt die Identität einer Person. Es wird also überprüft, ob die aktuell aufgenommenen und daraus errechneten Daten mit den gespeicherten Daten identisch sind. Bei der Identifikation erfolgt ein Abgleich der aktuell aufgenommenen Daten mit einer Vielzahl von Datensätzen, die in einer Datenbank abgelegt sind.[2]

Nach § 4 Abs. 3 Passgesetz wird eine bundesweite Datei untersagt. Bei der Kontrolle erfolgt daher nur eine Verifikation, ob die den Pass vorlegende Person mit dem Passinhaber identisch ist.

4.2.2 Biometrie im Kampf gegen den Terrorismus

Da jeder Mensch über einzigartige Merkmale verfügt, über die er sich eindeutig identifizieren lässt, setzen Politiker auf die Biometrie, um potenzielle Terroristen möglichst frühzeitig erkennen zu können.

Werden Terroristen oder Verbrecher erkannt, bevor sie ihre geplanten Anschläge verüben, können sie keinen Schaden mehr anrichten.

---

[1] Schaar, 76 f.
[2] Schaar, 79.

Vorraussetzungen für eine frühzeitige Enttarnung können unter anderem fälschungssichere Ausweispapiere sein. Wird der Inhaber eines Ausweises zusätzlich auf der Fahndungsliste aufgeführt, so besteht die Möglichkeit, ihn bei Grenzkontrollen zu erkennen und festzunehmen.[1]

Ziel ist es also, die Ausweisinhaber zweifelsfrei identifizieren zu können. Doch wie wird „zweifelsfrei" definiert? Sicher ist, dass biometrische Systeme Personen nicht zu 100 Prozent erkennen können, da die Daten bei jeder Eingabe geringfügig anders sind. Das System muss daher eine gewisse Toleranz aufweisen. Der europäische Standard für Zugangskontrollen EN 50133-1 verlangt eine Falschakzeptanzrate von 0,001 Prozent und eine Falschzurückweisungsrate von weniger als einem Prozent. Die Falschakzeptanzrate bezieht sich darauf, dass das System nicht erkennt, dass Person und Ausweis nicht zueinander gehören. Für die Praxis problematisch sind aber die hohen Falschzurückweisungsraten. In diesem Fall erkennt das System nicht, dass Person und Ausweis zueinander gehören.[2] Würden am Flughafen in Frankfurt mit 54 Millionen Fluggästen im Jahr 2007[3] ein Prozent der Passagiere falsch zurückgewiesen, so müsste man dort täglich mit etwa 1.500 Fehlalarmen umgehen. Biometrische Systeme können also keinesfalls eine Person zweifelsfrei identifizieren.

Sind Attentäter und Kriminelle außerdem noch nicht aufgefallen oder reisen sie unter richtigem Namen, so können sie durch eine Identitätskontrolle nicht entdeckt werden.[4]

Unter Berücksichtigung all dieser Tatsachen ist es wohl eher der psychologische Effekt, als die technische Leistungsfähigkeit, die etwas mehr Sicherheit bringen könnte, indem durch das bloße Vorhandensein solcher Systeme viele Betrüger abgeschreckt werden.[5] Dies ist jedoch nicht die eigentliche Zielgruppe, für die die Biometrie eingeführt wurde. Es

---

[1] Schulzki-Haddouti, 59.
[2] Schulzki-Haddouti, 68.
[3] Frankfurt Airport, siehe Anlage 9, 1.
[4] Schulzki-Haddouti, 59.
[5] Schulzki-Haddouti, 72.

ist davon auszugehen, dass Terroristen einen Weg finden werden, diese zu überwinden.

4.2.3 Biometrie aus datenschutzrechtlicher Sicht

Die besondere Gefährdung des Datenschutzes wird beim Thema Biometrie darin gesehen, dass die biometrischen Angaben nicht nur zur Personenerkennung eingesetzt werden können, sondern zusätzliche höchstpersönliche Informationen enthalten. Allein für die Entscheidung, ob es sich um eine bestimmte Person handelt, werden vergleichsweise viele Daten erhoben, die zu diesem Zweck nicht benötigt werden, aber weitere Auswertungsmöglichkeiten bieten. Bei spezieller Haar- und Barttracht oder Kopfbedeckungen kann zum Beispiel auf die Religionszugehörigkeit geschlossen werden. Außerdem könnte die Auswertung der erfassten Merkmale durch zukünftige Erkenntnisse zum Beispiel in der Genetik verbessert werden und so vielleicht aus Fingerabdrücken auf genetisch bedingte Krankheiten geschlossen werden.

All diese im „ePass“ gespeicherten Daten der Reisenden können Behörden in aller Welt auslesen und es besteht keine Möglichkeit, die weitere Verarbeitung und Nutzung zu kontrollieren.

Auch besteht die Gefahr, dass die Daten, die für den Zweck der Verifikation erhoben wurden, Begehrlichkeiten für andere Zwecke wecken. Zu denken wäre hier beispielsweise an die Strafverfolgung. Zwar ist eine anderweitige Verwendung bisher noch nicht möglich, da die Daten nicht zentral gespeichert werden. Aber durch eine Gesetzesänderung könnte dies schnell geändert werden.[1]

So ist jetzt bereits in § 22a Passgesetz geregelt, dass die digitalisierten Lichtbilder aus den Passregistern zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten abgerufen werden dürfen.

Bemerkenswert in dieser Hinsicht ist die in den 1980er Jahren geführte Debatte um den „maschinenlesbaren fälschungssicheren

[1] Schaar, 80 ff.

Personalausweis“. Sie war eine Reaktion auf den Terrorismus der Roten-Armee-Fraktion. Aufgrund des Volkszählungsurteils wurde damals im Passgesetz das ausdrückliche Verbot aufgenommen, Fingerabdrücke in den Personalausweis aufzunehmen.[1] Kritiker meinen, dass man den Parlamenten und der Öffentlichkeit vor der Verabschiedung des Terrorismusbekämpfungsgesetzes mehr Zeit hätte lassen müssen, damit sie sich der Tragweite der Grundrechtseingriffe im Zusammenhang mit dem zu erwartenden Nutzen hätten bewusst werden können. Auch hätten zum Beispiel Mängel bei den Sicherheitsbehörden aufgedeckt werden müssen. Denn wer neue Befugnisse zur Strafverfolgung und Gefahrenabwehr wolle, müsse begründen, warum er mit den bestehenden Befugnissen nicht ausgekommen ist.[2]

Die Einführung der biometrischen Daten erfolgte jedoch letztendlich aufgrund der oben genannten EG-Verordnung, weshalb im Folgenden deren Verhältnismäßigkeit überprüft werden soll.

4.2.4 Verhältnismäßigkeit der EG-Verordnung

Staatliche Eingriffe müssen dem Grundsatz der Verhältnismäßigkeit entsprechen. Das bedeutet, sie müssen geeignet, erforderlich und angemessen sein. Dies gilt auch für die Erhebung und Verarbeitung personenbezogener Daten.

Laut EG-Verordnung dient die Einführung biometrischer Daten dem Ziel, Pässe vor Fälschung zu schützen und eine verlässliche Verbindung zwischen dem Dokument und dessen rechtmäßigem Inhaber herzustellen.[3] Personen mit gefälschtem oder falschem Pass sollen dadurch geringere Chancen bekommen, in ein Land einzureisen.

Biometrische Merkmale sind grundsätzlich dazu geeignet festzustellen, ob der berechtigte Ausweisinhaber und der derzeitige Inhaber identisch sind.

---

[1] Schaar 138 f.
[2] Schaar, 139.
[3] ABl. EG Nr. L 385, 1.

Daher ist die Maßnahme, biometrische Merkmale in Pässe aufzunehmen, geeignet, das oben genannte Ziel zu erreichen.[1]

Bei der Erforderlichkeitsprüfung ist zu beachten, dass das mildeste geeignete Mittel angewandt wird. Biometrische Daten sind einzigartig, unveränderlich und lebenslang an eine Person gebunden. Zur Identifikation einer Person sind sie also prädestiniert. Allerdings können diese Merkmale, im Gegensatz zu nicht-biometrischen Merkmalen wie zum Beispiel dem Namen, Passwörtern oder Kennnummern, auch nicht einfach geändert werden. Außerdem werden sie von den Betroffenen bei vielen Gelegenheiten unbeabsichtigt zurückgelassen (z.B. Fingerabdruck). Grundsätzlich wäre daher der Einsatz von nicht-biometrischen Merkmalen das mildere Mittel.[2] Da bei nicht-biometrischen Merkmalen aber nicht ausgeschlossen ist, dass andere Personen dieses Merkmal für sich verwenden, kann keine verlässliche Personenbindung hergestellt werden.[3] Das eigentlich mildere Mittel scheidet deshalb aufgrund fehlender Geeignetheit aus.

Je mehr biometrische Daten erhoben werden, desto schwerer ist der Eingriff in das Recht auf informationelle Selbstbestimmung. Die Begrenzung auf ein Merkmal wäre also das mildere Mittel. Ob Systeme mit mehreren Merkmalen wirksamer sind, als Systeme mit nur einem Merkmal, ließe sich erst durch statistische Erhebungen ermitteln. Denn je mehr Merkmale involviert sind, desto höher ist auch die Fehlerwahrscheinlichkeit. Eindeutige Zahlen hierzu liegen jedoch nicht vor. Da aber der Wortlaut der Artikel 7 und 8 des Terrorismusbekämpfungsgesetzes, sowie der ursprüngliche Entwurf der EG-Verordnung lediglich die Aufnahme eines biometrischen Merkmals vorsahen, wurde hier wohl zunächst die Aufnahme eines zweiten Merkmals nicht als erforderlich betrachtet. An der Erforderlichkeit von

---

[1] Pallasky, 53 f.
[2] Pallasky, 54 f.
[3] Pallasky, 32.

mehreren Merkmalen bestehen daher erhebliche Zweifel, da noch nicht erwiesen ist, dass diese auch leistungsfähiger sind.[1]

Die generelle Auswahl von Gesichtsbild und Fingerabdruck war insoweit erforderlich, als andere Verfahren einen zu geringen Entwicklungsstand aufweisen und daher weniger leistungsfähig sind.[2]

Weiterhin ist zu prüfen, ob der Eingriff in die Rechte der Betroffenen angemessen ist, das heißt er darf nicht außer Verhältnis zum angestrebten Erfolg stehen. Hier gilt es also, dem Eingriff in das informationelle Selbstbestimmungsrecht das Gewicht und die Dringlichkeit der Gefahrenabwehr gegenüberzustellen.[3]

Die Aufnahme biometrischer Daten in die Reisepässe stellt einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar. Denn diese Daten enthalten neben den zur Identifikation benötigten Informationen noch viele zusätzliche, die zum Beispiel Rückschlüsse auf die religiöse Gesinnung zulassen. Diese Daten können künftig in allen Ländern, ungeachtet ihres Datenschutzniveaus, ausgelesen, gespeichert und verarbeitet werden. Der Betroffene kann nicht mehr überblicken, was mit seinen Daten geschieht.[4]

Weitere Gefahren für die Daten auf den Chips bestehen auch durch unbefugtes Auslesen oder durch das Abhören einer stattfindenden Kommunikation zwischen Chip und Lesegerät. Hier gilt es, mit technischen Sicherheitsvorkehrungen wirksam entgegen zu wirken.

Der Eingriff erfolgt zugunsten der Gefahrenabwehr. Das Ziel der Verbesserung der Grenzsicherheit kann nur dadurch erreicht werden, dass das System eine möglichst geringe Anzahl von Personen fälschlicherweise akzeptiert. Dies führt jedoch dazu, dass vermehrt berechtigte Personen zurückgewiesen werden. Diese müssen dann entgegen der Vermutung des biometrischen Systems darlegen, dass sie „sie selbst“ sind. Dabei könnte es schwierig werden, das Vorliegen eines

---

[1] Pallasky, 61 ff.
[2] Pallasky, 65.
[3] Pallasky, 67.
[4] Pallasky, 68.

Fehlers nachzuweisen, denn bei der automatisierten biometrischen Erkennung wird von einer größeren Fehlerfreiheit ausgegangen, die es erst einmal zu widerlegen gilt.
Diesem Problem kann nur durch eine Absenkung der Toleranzschwelle abgeholfen werden, was allerdings zur Folge hat, dass die Sicherheit herabgesetzt wird.[1]
Angemessen ist der Eingriff auch nur dann, wenn er gerechtfertigt ist. Dazu müsste die bisherige Sicherheit von Reisepässen unzureichend sein. Dafür gibt es jedoch keinerlei Anhaltspunkte.[2] Die bisherigen Pässe zählen laut Angaben der Bundesdruckerei zu den sichersten der Welt.[3]
Das eigentliche Problem und damit die Gefahr für die Sicherheit entsteht durch die Verwendung echter Pässe mit einer erschlichenen Identität. Durch Bestechung oder Erpressung können Pässe produziert werden, die biometrische Merkmale mit einem falschen Namen verbinden. Da biometrische Verfahren den Anschein größerer Fehlerfreiheit haben, wird es durch den Einsatz biometrischer Verfahren sogar schwerer, Fälschungen nachzuweisen. Eine wesentliche Verbesserung der Grenzsicherheit ist daher nicht zu erwarten. Lediglich im Bereich der mittelschweren Kriminalität könnte ein Erfolg zu erwarten sein, jedoch nicht im Bereich des Terrorismus. Denn biometrische Pässe können Personen nicht enttarnen, die den Sicherheitsbehörden bisher nicht bekannt waren und die ihre wirkliche Identität benutzen. Bei den meisten Terroristen dürfte dies der Fall sein.
Der relativ geringe Sicherheitsgewinn steht nicht in einem angemessenen Verhältnis zur Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung. Daher entspricht die Aufnahme der biometrischen Merkmale in Reisepässen nicht dem Grundsatz der Verhältnismäßigkeit.[4]
Trotzdem entfaltet die EG-Verordnung ihre volle rechtliche Wirkung. Um die Auswirkungen für die Zukunft so gering wie möglich zu halten, sollte

---

[1] Pallasky, 69 ff.
[2] Pallasky, 74.
[3] Bundesdruckerei, siehe Anlage 10, 1.
[4] Pallasky, 74 ff.

darauf geachtet werden, dass eine zentrale Biometrie-Datenbank unbedingt verhindert wird und dass die biometrischen Daten tatsächlich nur zur Verifikation von Reisenden verwendet werden. Außerdem sollte man die internationale Standardisierung der Speicherung biometrischer Merkmale als so genannte Templates vorantreiben.[1] Templates sind Datensätze, die nach einer bestimmten Methode aus den Volldatensätzen der biometrischen Merkmale extrahiert werden. Sie enthalten weniger Informationen über die jeweilige Person als die bisher gespeicherten Rohdaten und sind daher datenschutzrechtlich wegen des Grundsatzes der Datensparsamkeit zu bevorzugen.[2]

4.3 Die Vorratsdatenspeicherung

Am 01. Januar 2008 traten die Regelungen zur Vorratsdatenspeicherung in Deutschland in Kraft. Der Deutsche Bundestag hatte das entsprechende „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“[3] am 21. Dezember 2007 verabschiedet.

Durch dieses Gesetz wurde das Telekommunikationsgesetz dahingehend geändert, dass nun Telekommunikations-Dienstleister verpflichtet sind, die bei der Nutzung ihres Dienstes erzeugten oder verarbeiteten Verkehrsdaten von allen Benutzern für sechs Monate zu speichern (§ 113 a Abs. 1 TKG). Als Verkehrsdaten gelten zum Beispiel Rufnummern, Beginn und Ende der Verbindung sowie bei mobilen Telefondiensten auch Standortdaten (§ 113 a Abs. 2 TKG). Bei Versenden einer elektronischen Nachricht werden die Daten des Absenders und die des Empfängers, sowie der Zeitpunkt der Nutzung gespeichert (§ 113 a Abs. 3 TKG). Einzig

---

[1] Pallasky, 80.
[2] Roßnagel/Hornung, DÖV 2005, 983, 985.
[3] BGBl. I 2007, 3198 ff.

und allein der Inhalt der Kommunikation darf nicht gespeichert werden (§ 113 a Abs. 8 TKG).

Diese auf Vorrat gespeicherten Daten sollen zur Verfolgung von Straftaten, zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit und zur Erfüllung nachrichtendienstlicher Aufgaben des Verfassungsschutzes, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes verwendet werden. Zu diesen Zwecken dürfen die Daten an die zuständigen Stellen auf Verlangen und bei Vorliegen einer Einzelfallanordnung übermittelt werden (§ 113 b TKG).

4.3.1 Entwicklung der Regelungen

Schon bisher war es den Telekommunikations-Dienstleistern erlaubt, die Daten, die sie für die Abrechnung benötigten, bis zu sechs Monate nach dem Versand der Rechnung aufzubewahren. Verkehrsdaten, die jedoch nicht zu Abrechnungszwecken benötigt wurden, waren sofort zu löschen (§ 97 Abs. 3 TKG in der Fassung von 2004).

Gemäß § 100 g StPO konnte im Strafverfahren angeordnet werden, dass Anbieter Verkehrsdaten herausgeben mussten, wenn jemand im Verdacht stand, eine bestimmte Straftat begangen zu haben. Auch die Geheimdienste konnten unter bestimmten Voraussetzungen nach dem G-10-Gesetz die Herausgabe von Verkehrsdaten beantragen. Hierbei konnten jedoch selbstverständlich nur Daten herausgegeben werden, die zum Zwecke der Abrechnung noch vorhanden waren.[1]

Bereits im Jahr 2002 wurde in Deutschland auf Initiative des Bundesrats über eine Speicherung von Telekommunikationsdaten auf Vorrat diskutiert. Dies wurde damals von der Bundesregierung mit dem Hinweis auf entgegenstehende grundgesetzliche Erwägungen abgelehnt.[2] Auch

---

[1] Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, DuD 2004, 603, 604.

[2] BT-Dr 14/9801, 15.

durch die Verabschiedung des novellierten Telekommunikationsgesetzes im Jahr 2004 änderte sich an dieser Situation nichts.[1]

Die entscheidende Wende brachte der Erlass der EG-Richtlinie 2006/24/EG. Auf europäischer Ebene wurde bereits seit den Terroranschlägen des 11. Septembers 2001 in den USA und den Anschlägen von Madrid im Jahr 2004 über Pläne zur Vorratsdatenspeicherung diskutiert. Die bei der Nutzung elektronischer Kommunikationsmöglichkeiten anfallenden Daten wurden als wichtige und nützliche Mittel zur Aufklärung und Ahndung von Straftaten angesehen. Zu einer Entscheidung konnte man sich allerdings erst im Jahr 2005 durchringen und die damals angenommene Richtlinie wurde am 15. März 2006 verabschiedet.[2]

Diese Richtlinie wurde in Deutschland durch das bereits genannte „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ in nationales Recht umgesetzt.

4.3.2 Rechtliche Würdigung in Bezug auf den Datenschutz

Die zahlreichen Stellungnahmen zu diesem Gesetz sind sich im Wesentlichen darin einig, dass diese Regelungen nicht mit deutschem Recht zu vereinbaren sind.

Das Bundesverfassungsgericht stellte schon im Volkszählungsurteil von 1983 klar, dass bereits die Erhebung und Speicherung personenbezogener Daten einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt. Solche Eingriffe sind nur mit einer gesetzlichen Grundlage zulässig, die dem Grundsatz der Verhältnismäßigkeit entspricht.[3]

Danach ist also die Norm zunächst daraufhin zu prüfen, ob sie geeignet ist, ihren Zweck zu erfüllen. Als Zweck wird hier die Verbesserung der

---

[1] Hülsmann, DuD 2004, 734.
[2] Leutheusser-Schnarrenberger, ZRP 2007, 9 f.
[3] BVerfG, BVerfGE 65, 1.

Strafverfolgung genannt. Nun stellt sich allerdings die Frage, ob es nicht gerade potentiellen Tätern ohne größere Anstrengungen möglich ist, einer Entdeckung mittels Vorratsdatenspeicherung zu entgehen. So kann zum Beispiel durch Nutzung von öffentlichen Telefonzellen, durch ständiges Wechseln des Mobiltelefons oder durch Fälschung von elektronischen Adressen im Internet eine Rückverfolgung durch die Strafverfolgungsbehörden leicht verhindert werden.[1] Es ist davon auszugehen, dass die Gefahr von Umgehungen umso größer wird, je besser die Tat geplant ist. Durch die Vorratsdatenspeicherung sollen jedoch gerade die organisierte Kriminalität und der Terrorismus bekämpft werden.[2]

Bedenkt man ferner die Datenmenge, die durch die weite Verbreitung von Internet, Mobiltelefon und herkömmlichem Telefon heutzutage anfällt, so ist fraglich, ob eine zielführende Auswertung der Daten überhaupt möglich ist. Das zu speichernde Datenvolumen eines großen Internetanbieters beläuft sich auf 20.000 bis 40.000 Terabyte. Dies entspricht ungefähr vier Millionen Kilometer gefüllter Aktenordner. Ohne zusätzliche Investitionen würde ein einmaliger Suchlauf mit der vorhandenen Technik 50 bis 100 Jahre dauern. Selbst mit technischer Aufrüstung ist daher eine rasche Verfügbarkeit der Daten zu bezweifeln.[3] Durch die gewaltigen Massen an nicht notwendigen Daten, die bei einer Speicherung auf Vorrat anfallen, ist davon auszugehen, dass kein wesentlicher Sicherheitsgewinn erzielt werden kann.[4] Auch kann hier nicht von einer präventiven Wirkung im Bereich der Gefahrenabwehr (§ 113 b Nr. 2 TKG) gesprochen werden, da die Vorratsdatenspeicherung vergangenheitsbezogen ist und somit lediglich bei der Aufklärung bereits begangener Straftaten behilflich sein könnte.[5] Es ist daher festzuhalten, dass an der Geeignetheit dieser Regelungen gezweifelt werden darf.

---

[1] Ulmer/Schrief, DuD 2004, 591, 595.
[2] Gola/Klug/Reif, NJW 2007, 2599.
[3] Europäisches Parlament, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, siehe Anlage 11, 2 ff.
[4] zit. nach Gola/Klug/Reif, NJW 2007, 2599, 2600.
[5] Leutheusser-Schnarrenberger, ZRP 2007, 9, 11.

Ein weiterer Aspekt des Verhältnismäßigkeitsgrundsatzes ist die Erforderlichkeit. Es ist zu prüfen, ob nicht ein milderes Mittel vorhanden ist, durch welches die Betroffenen weniger beeinträchtig werden würden. Als milderes Mittel ist hier das so genannte „Quick freeze"-Verfahren zu nennen. Dieses Verfahren ist zum Beispiel in § 16 b des Wertpapierhandelsgesetzes geregelt und wird in diesem Bereich bereits angewandt. Bei einem konkreten Tatverdacht können Behörden die Datenlöschung blockieren und die vorhandenen Daten werden „eingefroren". Durch eine richterliche Anordnung werden diese Daten „aufgetaut" und den Behörden zur Verfügung gestellt.[1] Dies ist ein wesentlich milderes Mittel gegenüber der Datenspeicherung auf Vorrat, da hier für die Speicherung ein konkreter Tatverdacht vorliegen muss und nicht von vornherein alle Bürger unter Generalverdacht gestellt werden. Außerdem besteht der Vorteil einer anlassbezogenen Speicherung darin, dass nicht riesige Datenmengen, sondern nur Daten bestimmter auffälliger oder verdächtiger Personen mit deutlich geringerem Aufwand gespeichert und ausgewertet werden müssen.[2]

Weitere Zweifel an der Erforderlichkeit der Vorratsdatenspeicherung über sechs Monate lassen auch Analysen schwedischer und britischer Stellen aufkommen. Diese besagen, dass sich Datenabfragen von Behörden in den Ländern, in denen die Vorratsdatenspeicherung bereits praktiziert wird, zu 80 bis 85 Prozent auf die letzten drei Monate beziehen. Statistische Angaben aus den Niederlanden und Österreich besagen, dass Verkehrsdaten nur einen geringen Beitrag zur Strafverfolgung leisten. Denn von den Behörden würden meist nur Bestandsdaten (Name, Adresse, Kennungen) abgefragt.[3] So ist auch die Erforderlichkeit nicht zweifelsfrei bewiesen.

Der letzte Prüfschritt der Verhältnismäßigkeit ist die Angemessenheit. Danach darf kein Nachteil herbeigeführt werden, der erkennbar außer Verhältnis zum beabsichtigten Erfolg steht. Da heutzutage nahezu jede

---

[1] Bizer, DuD 2002, 363.
[2] Bundesverband der Deutschen Industrie, DuD 2004, 606, 607.
[3] Büllingen, DuD 2005, 349, 351.

Person an der elektronischen Kommunikation teilnimmt und dabei eine große Menge an Datenspuren erzeugt, ist von der Vorratsdatenspeicherung fast jeder unmittelbar betroffen. Außerdem handelt es sich um eine verdachtslose Maßnahme, in die fast ausschließlich solche Personen einbezogen sind, die sich keinerlei Fehlverhalten vorwerfen lassen müssen und die den Eingriff in ihre Grundrechte durch ihr Verhalten nicht veranlasst haben. Berücksichtigt man zusätzlich, dass der beabsichtigte Erfolg, nämlich die abzuwehrende Bedrohung für die öffentliche Sicherheit, nicht konkretisierbar ist und man auch nicht sagen kann, ob diese Regelungen irgendwann einen Nutzen haben werden, ist davon auszugehen, dass der Eingriff in das Grundrecht auf informationelle Selbstbestimmung nicht angemessen ist.[1]

In seinem Urteil von 1983 führte das Bundesverfassungsgericht aus, dass man zur Abgabe von personenbezogenen Daten nur gezwungen werden kann, wenn der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt. Damit sei, so das Bundesverfassungsgericht, eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren.[2]

Die pauschale Formulierung „zur Verfolgung von Straftaten“ in § 113 b Nr. 1 TKG, wird diesem Bestimmtheitsgrundsatz nicht gerecht. Die Effektivität der Verbrechensbekämpfung an sich kann keine legitime Rechtfertigung von Eingriffen in Rechtspositionen darstellen, da dies zu Maßlosigkeit führen würde. Hier wäre eine exakte Bestimmung der Straftatbestände erforderlich, die einen Datenzugriff rechtfertigen würden.[3]

Die Regelungen zur Vorratsdatenspeicherung stehen in einem klaren Gegensatz zu dem aus dem Recht auf informationelle Selbstbestimmung abgeleiteten und in § 3 a BDSG verankerten Grundsatz der Datenvermeidung und Datensparsamkeit.

---

[1] Leutheusser-Schnarrenberger, ZRP 2007, 9, 11.
[2] BVerfG, BVerfGE 65, 1, 46.
[3] Gola/Klug/Reif, NJW 2007, 2599.

Daher ist festzustellen, dass die Regelungen zur Vorratsdatenspeicherung in Deutschland nicht grundgesetzkonform sind.[1]

4.3.3 Datenschutz als Hindernis für die Sicherheit?

Wenn man es genau nimmt, hätte die Vorratsdatenspeicherung, wie oben dargelegt, in Deutschland nicht eingeführt werden dürfen, da dies dem geltenden Datenschutzrecht widerspricht.
So könnte zu recht der Gedanke aufkommen, dass der Datenschutz ein Hindernis beim Schutz der inneren Sicherheit der Bundesrepublik darstellt. Doch wie es im Recht üblich ist, wenn sich zwei Positionen gegenüber stehen, ist abzuwägen, welche Seite schwerer wiegt. Eine Seite muss dann gegebenenfalls Kompromisse hinnehmen.
Leider war und ist meist der Datenschutz die Seite, die Kompromisse hinnehmen muss, da auf der anderen Seite häufig die Sicherheit der Allgemeinheit steht und diese höher eingestuft wird.
Jedoch muss speziell bei der Vorratsdatenspeicherung beachtet werden, dass es sich um einen großen Eingriff in den Datenschutz handelt, da alle Menschen, ob schuldig oder nicht, davon betroffen sind.
Das Datenschutzrecht der Bundesrepublik ist nicht umsonst so, wie es heute ist. Im Hinblick auf eine funktionierende Demokratie ist dies unumgänglich. In einer demokratischen Gesellschaft kann es nicht zulässig sein, dass das gesamte elektronische Kommunikationsverhalten systematisch registriert wird.[2]
Außerdem ist bei jeder Abwägung zu bedenken, dass Grundrechtspositionen selten wieder aufgewertet werden, wenn sie einmal eingeschränkt wurden.[3]

---

[1] Leutheusser-Schnarrenberger, ZRP 2007, 9, 11.
[2] Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, DuD 2004, 603, 605.
[3] Gola/Klug/Reif, NJW 2007, 2599, 2601.

4.4 Übermittlung von Fluggastdatensätzen in die USA

Am 20. Dezember 2007 verabschiedete der Bundestag das „Gesetz zu dem Abkommen vom 26. Juli 2007 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (PNR-Abkommen 2007)“[1]. Darin stimmt der Bundestag dem genannten Abkommen zu.

Das Abkommen regelt die Übermittlung von Fluggastdaten bei Passagierflügen in die USA, aus den USA heraus oder durch die USA und deren Verwendung. Danach darf die amerikanische Grenzschutzbehörde bei europäischen Fluggesellschaften die Daten erheben, die in deren Reservierungs- und Buchungssystemen gespeichert sind. Darunter fallen zum Beispiel der Buchungscode, die betreffenden Namen, das Datum der Reservierung, die geplanten Abflugdaten, Vielflieger- und Bonusdaten, alle verfügbaren Kontaktinformationen, Zahlungs- und Abrechnungsinformationen, Informationen zum Gepäck, Sitzplatzinformationen und noch einiges mehr.[2] Die Daten werden erstmals 72 Stunden vor dem geplanten Abflug an die amerikanische Behörde übermittelt und bei Bedarf aktualisiert.[3] Die übermittelten Daten bleiben sieben Jahre lang in einer aktiven analytischen Datenbank gespeichert. Danach werden sie für acht Jahre in einen ruhenden Status transferiert. Auf diese ruhenden Daten kann nur unter bestimmten Voraussetzungen zugegriffen werden.[4]

4.4.1 Entwicklung

Diese Regelungen gehen auf die in den USA nach dem 11. September 2001 erlassenen Terrorismusbekämpfungsgesetze zurück. Sie enthielten

---

[1] BGBl. II 2007, 1978 ff.
[2] BGBl. II 2007, 1978, 1983 f.
[3] BGBl. II 2007, 1978, 1986.
[4] BGBl. II 2007, 1978, 1985.

die Verpflichtung für europäische Fluggesellschaften, der amerikanischen Grenzschutzbehörde bei Flügen in die USA, aus den USA heraus oder durch die USA einen elektronischen Zugriff auf die Passagierdatensätze zu gewähren, die in ihren Reservierungs- und Buchungssystemen gespeichert sind. Die Auswertung dieser so genannten PNR-Daten („Passenger Name Records“ = Passagierdatensätze) soll es den amerikanischen Sicherheitsbehörden ermöglichen, bereits vor dem Abflug gefährliche Personen zu identifizieren.[1] Da die USA den Fluggesellschaften Sanktionen angedroht hatten, wenn die Daten nicht zur Verfügung gestellt würden, wurde der Zugriff auf die Reservierungsdatenbanken nach inoffizieller Absprache zwischen den USA und der EU-Kommission seit März 2003 gewährt. Nachdem dies bekannt wurde, regte sich Widerstand auf europäischer Ebene. Zwar wurden bereits seit 1988 vor Abflug Angaben über Flug und Identität des Reisenden an die amerikanischen Sicherheitsbehörden übermittelt, der nun ermöglichte Zugriff auf die Passagierdatensätze ging jedoch weit darüber hinaus. Daher wurde von der EU-Datenschutzgruppe und dem EU-Parlament gefordert, die Übermittlung der Passagierdaten verbindlich, auch im Hinblick auf das geltende EU-Datenschutzrecht, zu regeln.[2] So trat die EU-Kommission in Verhandlungen mit der US-Regierung, um ein angemessenes Datenschutzniveau für die PNR-Daten zu schaffen.

Im Mai 2004 schloss der Rat der Europäischen Union mit den USA ein Abkommen, das die Fluggesellschaften rechtlich verpflichtet, die in ihren Reservierungs- und Buchungssystemen enthaltenen Daten für die US-Grenzschutzbehörde zum Abruf bereit zu halten. Diese Verpflichtung besteht jedoch nur, solange ein angemessenes Datenschutzniveau gewährleistet ist, welches in einer Verpflichtungserklärung der US-Grenzschutzbehörde festgehalten ist.[3] Auf Grundlage dieser

---

[1] Pallasky, 81 f.
[2] Pallasky, 83.
[3] Pallasky, 85.

Verpflichtungserklärung stellte die EU-Kommission die Angemessenheit des Datenschutzniveaus fest.[1]
Mit seinem Urteil vom 30. Mai 2006 erklärte der Europäische Gerichtshof sowohl den Beschluss des EU-Rates über den Abschluss des Abkommens von 2004, als auch die Angemessenheitsentscheidung der Kommission aufgrund einer falschen Rechtsgrundlage für nichtig.[2] Daher wurde eine Neuregelung, wie sie im Jahr 2007 vorgenommen wurde, notwendig.

4.4.2 Datenschutzrechtliche Sicht

Kritik an diesen Regelungen besteht hauptsächlich in Bezug auf das Datenschutzniveau der USA, an der Anzahl der übermittelten Daten und an einer vagen Zweckbestimmung seitens der USA, welche auch eine Weiterleitung an andere amerikanische Behörden ermöglicht.

Die Übermittlung von personenbezogenen Daten in Drittstaaten ist in Artikel 25 der EG-Datenschutzrichtlinie (95/46/EG)[3] geregelt. Eine Übermittlung ist danach nur zulässig, wenn dieses Land über ein angemessenes Datenschutzniveau verfügt. Dies ist nur dann der Fall, wenn die Anforderungen, die die Datenschutzrichtlinie an die Verwendung personenbezogener Daten stellt, gleichwertig erfüllt werden.[4]
Problematisch ist zum einen die Zweckbestimmung der PNR-Daten. Als Zweck der Datenerhebung wird die Verhütung und Bekämpfung des Terrorismus und damit verbundener Straftaten, sowie sonstiger schwerer grenzüberschreitender Straftaten und der Flucht vor Haftbefehlen und Gewahrsamnahme im Zusammenhang mit diesen Straftaten genannt.[5] Eine zu abstrakte Zweckbestimmung ist mit der Anforderung einer Zweckbindung der Daten nicht zu vereinbaren, da dann das Recht auf

---

[1] ABl. EG Nr. L 235, 11 ff.
[2] EuGH, NJW 2006, 2029 ff.
[3] ABl. EG Nr. L 281, 31 ff.
[4] Pallasky, 92.
[5] BGBl. II 2007, 1978, 1982.

informationelle Selbstbestimmung des Betroffenen besonderen Gefahren ausgesetzt ist. Für den Betroffenen muss eindeutig erkennbar sein, für welche Zwecke seine Daten bestimmt sind.
Diese Zweckbestimmung, die bereits in der oben genannten Verpflichtungserklärung enthalten war, wurde damals schon von einigen Kritikern als zu unbestimmt angesehen.[1] Denn es fehlt zum Beispiel eine Definition dessen, was Terrorismus bedeutet oder auch, zur Verfolgung welcher Straftaten die Daten verwendet werden können. Bedenklich ist in diesem Zusammenhang auch, dass den amerikanischen Behörden weit reichende Befugnisse zustehen, zur Gefahrenabwehr auf US-Datenbestände zuzugreifen. So kann zum Beispiel mit Hilfe der E-Mail-Adresse eines Fluggastes auf dessen E-Mail Konto zugegriffen werden, um nach verdächtigen E-Mails zu suchen. Mit der Kreditkartennummer können zurückliegende Transaktionen angefordert werden. In Zusammenhang mit der weiten Zweckbestimmung kann der Betroffene kaum noch überschauen, wer Kenntnis von seinen Daten hat und zu welchem Zweck sie verarbeitet werden.[2]

Die PNR-Daten können von der US-Grenzschutzbehörde an andere Behörden und sogar Drittstaaten weitergegeben werden.[3] Voraussetzung dafür ist, dass die Behörden Aufgaben im Bereich der Strafverfolgung, der öffentlichen Sicherheit und der Terrorismusbekämpfung innehaben. Sie sollen durch die Daten in ihren Ermittlungen unterstützt werden. Bei der Übermittlung an Drittstaaten ist zuvor der Schutz der Informationen beim Empfänger zu prüfen. Die Übermittlung von personenbezogenen Daten an Dritte birgt die Gefahr, dass sie möglicherweise zu anderen Zwecken genutzt werden, als sie erhoben wurden.

Der Datenumfang und die Speicherungsfrist von insgesamt 15 Jahren entsprechen nicht dem Grundsatz der Erforderlichkeit. Denn die PNR-

---

[1] Pallasky, 94 ff.
[2] Pallasky, 97 ff.
[3] BGBl. II 2007, 1978, 1983.

Daten enthalten auch so genannte sensitive Daten. Dies sind zum Beispiel Angaben über Essenswünsche (z.B. koscheres Essen), sowie aufgrund von Krankheiten oder Behinderung (z.B. Rollstuhlbenutzung) zu treffende Vorkehrungen. Daraus kann auf den gesundheitlichen Zustand oder die Zugehörigkeit zu einer bestimmten Religionsgemeinschaft des Passagiers geschlossen werden. Diese Daten sind in Artikel 8 Abs. 2 der EG-Richtlinie 95/46/EG besonders geschützt[1]. Eine verdachtslose Übermittlung dieser Daten ist zur Verbrechensbekämpfung nicht erforderlich.[2] Die Notwendigkeit einer enormen Speicherdauer von insgesamt 15 Jahren erscheint nicht erforderlich, um eine Person eindeutig identifizieren zu können und unmittelbar zu entscheiden, ob es sich um eine gefährliche Person handelt.

Es ist durchaus nachzuvollziehen, dass in den USA seit dem 11. September 2001 ein erhöhtes Bedürfnis nach Sicherheit besteht. Dies schließt den Wunsch ein, dass die Fluggäste eindeutig identifiziert werden können. Zu einer sicheren Identifikation sind jedoch nicht diese Massen an Daten notwendig, wie sie den USA nach dem PNR-Abkommen zur Verfügung gestellt werden.[3] Der Betroffene verliert die Kontrolle über seine Daten, wodurch die Grundvoraussetzung des Rechts auf informationelle Selbstbestimmung nicht erfüllt ist. Er weiß nicht mehr „wer was wann über ihn weiß“ und ist daher in der freien Entfaltung seiner Persönlichkeit eingeschränkt[4]. Die Gefahrenabwehr und der Datenschutz sind hier nicht in einen angemessenen Ausgleich gebracht worden.[5]
Eine Maßnahme, die wenigstens etwas zur Verbesserung der Lage beiträgt ist, dass sich die USA darauf eingelassen haben, auf das so genannte „push“-Verfahren umzustellen. Das heißt, dass nicht mehr der direkte Zugriff auf die Systeme der Fluggesellschaften ermöglicht wird, sondern die entsprechenden Daten durch die Fluggesellschaften an die

[1] Pallasky, 103.
[2] Pallasky, 144.
[3] Schaar, 141.
[4] BVerfG, BVerfGE 65, 1, 43.
[5] Pallasky, 145.

US-Behörde übermittelt werden.[1] Weiter wäre auf eine präzise Zweckbestimmung der Daten hinzuwirken und der Umfang auf ein erforderliches Maß zu beschränken. Sensitive Daten sollten von der Übermittlung ausgeschlossen sein. Überdacht werden sollte auch die Aufbewahrungsdauer der Daten.

4.5 Die Online-Durchsuchung

Die so genannte Online-Durchsuchung ist seit dem 25. November 2006 ein Gegenstand der öffentlichen Diskussion.

In einem Ermittlungsverfahren wegen des Verdachts der Gründung einer terroristischen Vereinigung und anderer Straftaten, beantragte der Generalbundesanwalt beim Ermittlungsrichter des Bundesgerichtshofs eine verdeckte Online-Durchsuchung auf Grundlage der §§ 102 ff StPO. Dem Beschuldigten sollte ein Computerprogramm zugespielt werden, um die auf den Speichermedien des Computers abgelegten Dateien zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörde zu übertragen. Der Ermittlungsrichter lehnte dies mangels gesetzlicher Ermächtigungsgrundlage ab.[2] In seinem Beschluss vom 31. Januar 2007 bestätigte der 3. Strafsenat des BGH die Entscheidung, dass für eine auf heimliche Ausführung angelegte Durchsuchung zu Strafverfolgungszwecken keine Ermächtigungsgrundlage besteht.[3]

Bisher besteht lediglich zum Zweck der Aufklärung von Gefahren durch den Verfassungsschutz in Nordrhein-Westfalen eine solche Ermächtigung (§ 5 Abs. 2 Nr. 11 Verfassungsschutzgesetz NRW). Gegen diese Regelung ist jedoch eine Verfassungsbeschwerde anhängig. Eine Entscheidung des Bundesverfassungsgerichts, ob diese Regelung verfassungsgemäß ist, soll am 27. Februar 2008 fallen und kann daher in

---

[1] BGBl. II 2007, 1978, 1985.
[2] BGH, DuD 2007, 134.
[3] BGH, BGHSt 51, 211 ff.

dieser Arbeit nicht mehr berücksichtigt werden. Sie wird Auswirkungen auf eventuelle bundesweite Regelungen haben.

Nach der Entscheidung des BGH begann eine politische Debatte, ob die Online-Durchsuchung ein vertretbares Mittel zur Aufklärung von Straftaten sei und ob hierfür gesetzliche Rechtsgrundlagen geschaffen werden sollen.[1]

In seiner Rede anlässlich der Vorstellung des Verfassungsschutzberichts 2006 am 15. Mai 2007, betonte Bundesinnenminister Dr. Wolfgang Schäuble die Notwendigkeit von verdeckten Online-Durchsuchungen. Terroristische Aktivitäten würden immer mehr in die virtuelle Welt verlagert, so Schäuble. Man könne die Augen nicht vor den technischen Entwicklungen verschließen, denn „auf selbst verordnete Blindheit nehmen Terroristen keine Rücksicht“. Da es sich hierbei um eine sensible Materie handle, müsse eine verfassungsrechtlich einwandfreie und klare Regelung geschaffen werden. Falls notwendig auch durch eine Ergänzung des Grundgesetzes.[2]

Auch wird argumentiert, dass in Zeiten rasant zunehmender Technisierung, globaler terroristischer Verflechtungen und dem konspirativen Vorgehen der Gegenseite, die Strafverfolgungsbehörden nicht mit herkömmlichen Mitteln und Methoden „hinterherhinken“ könnten. Es sei nicht zu verantworten, die Sicherheit der Menschen durch Vernachlässigung zeitgemäßer Ermittlungsmethoden aufs Spiel zu setzen.[3]

4.5.1 Begriff und Technik

Unter dem Begriff Online-Durchsuchung versteht man das für den Nutzer verdeckte („heimliche“) Ausspähen und Kopieren der in einem Computersystem gespeicherten Daten durch staatliche Behörden über

---

[1] Roßnagel, DRiZ 2007, 229.
[2] Schäuble, siehe Anlage 12, 1.
[3] Hunsicker, Kriminalistik 2007, 187, 190.

einen Internetzugang.[1] Die Daten sollen gegebenenfalls als Beweismaterial beschlagnahmt werden.

Werden derzeit Daten von Computern als Beweismaterial herangezogen, werden in der Regel die ganzen Computer, zumindest aber deren Festplatten sichergestellt und von sachverständigen Kriminaltechnikern einer so genannten forensischen Analyse unterzogen. Dabei werden digitale Spuren und Beweise gesichert. Die jeweilige Festplatte wird schreibgeschützt ausgelesen. Außerdem wird eine Kopie in Form eines identischen Abbildes angefertigt, um zu verhindern, dass versteckte Dateien übersehen werden und um eine Veränderung des Untersuchungsgegenstands auszuschließen. Inhaltliche Untersuchungen werden stets an der Kopie und nicht am Originaldatenträger durchgeführt. Denn eine wesentliche Grundlage für die Revisionsfähigkeit und damit die Verlässlichkeit der Untersuchungsmethode ist der Beweis, dass der Originaldatenträger nicht verändert wurde.[2]

Es ist noch nicht erwiesen, ob ein solches revisionsfestes Beweiserhebungsverfahren auch bei der Durchsuchung von Systemen und der Beschlagnahme von Dateien mittels Online-Zugriff möglich ist.

Die Online-Durchsuchung besteht aus vier Schritten.

Zunächst muss das Zielsystem genau analysiert werden. Die Detailkenntnisse über die technischen Voraussetzungen auf dem Zielsystem sind für die Ausgestaltung und die erfolgreiche Installation der Durchsuchungssoftware unbedingt erforderlich.[3]

Dann muss auf dem zu untersuchenden System eine Software installiert werden, die den Ermittlern den Online-Zugriff per Internet ermöglicht. Diese Software nennt man „Trojanisches Pferd“. Sie kann über einen verdeckten Eingabekanal Handlungsanweisungen empfangen, über einen

---

[1] Hornung, DuD 2007, 575.
[2] Hansen/Pfitzmann, DRiZ 2007, 225.
[3] Fox, DuD 2007, 827, 828.

verdeckten Ausgabekanal Daten senden, in dem System selbst Daten gewinnen und auch manipulieren.[1]

Diese Installation eines „Trojanischen Pferdes“ nennt man Infiltration. Sie kann auf unterschiedliche Weise erfolgen. Dem Nutzer könnte zum Beispiel eine E-Mail zugesandt werden, die im Anhang mit einem „Trojanischen Pferd“ versehen ist. Durch das Öffnen der E-Mail und des Anhangs wird der „Trojaner“ aktiviert. Ebenso könnte dem Nutzer eine präparierte CD oder ein USB-Stick zugespielt werden, die Installationsdateien mit „Trojanischen Pferden“ enthalten. Hierbei muss der Nutzer jedoch immer einen Beitrag zur Infiltration leisten. Ohne Hilfe des Nutzers können „Trojaner“ zum Beispiel durch Sicherheitslücken in Programmen oder Betriebssystemen eingeschleust werden.

Das Risiko bei diesen Methoden besteht jedoch darin, dass nicht auszuschließen ist, dass ein anderes System als das der Zielperson mit dem „Trojanischen Pferd“ infiltriert wird und so in die Privatsphäre Unbeteiligter eingedrungen wird.[2] Dies kann zum Beispiel dann der Fall sein, wenn der Beschuldigte die E-Mail mit dem „Trojaner“ bei Bekannten oder am Arbeitsplatz abruft. Eine CD könnte der Beschuldigte weitergeben.[3] Die einzige Möglichkeit, dies auszuschließen wäre, heimlich in die Räumlichkeiten, in denen der Zielrechner steht, einzudringen und die Software direkt zu installieren.

Ohne einen direkten Zugriff auf den Rechner sind die Ermittler auf die gleichen Methoden wie Virenautoren angewiesen, weshalb mit aktiven Gegenmaßnahmen in Form von Anti-Viren-Software, Firewalls etc. gerechnet werden muss.[4]

Nach der Infiltration erfolgt im dritten Schritt die eigentliche Online-Durchsuchung. Die Ermittler können nun per Internet auf den Rechner zugreifen, sofern eine Online-Verbindung besteht, und können die dort vorhandenen Daten auslesen oder verändern. Durch vorgegebene Such-

---

[1] Hansen/Pfitzmann, DRiZ 2007, 225.
[2] Hansen/Pfitzmann, DRiZ 2007, 225, 227.
[3] Hornung, DuD 2007, 575, 579.
[4] Hansen/Pfitzmann, DRiZ 2007, 225, 227 f.

Kommandos kann eine Durchsuchung auch ohne Online-Verbindung automatisiert durchgeführt werden. Die so gewonnen Daten werden bis zur nächsten Online-Verbindung zwischengespeichert und dann an die Strafverfolgungsbehörden übertragen.[1] Eine Echtheitsbestätigung dieser übertragenen Daten kann jedoch nicht erfolgen, da nicht ausgeschlossen werden kann, dass Dritte, zum Beispiel über ein weiteres „Trojanisches Pferd“, gleichzeitig Kontrolle über das System ausüben und zu Täuschungszwecken auf den Rechner zugreifen.

Tastatureingaben, wie zum Beispiel Passworte können ebenfalls abgefangen werden. Besteht währenddessen keine Internetverbindung, können die Daten zwischengespeichert werden und bei der nächsten Verbindung zum Internet an die Ermittler weitergegeben werden. Dies beinhaltet jedoch zum einen eine Veränderung des Untersuchungsgegenstands und zum anderen eine Gefährdung des Nutzers, da ein unbefugter Zugriff auf das nun gespeicherte Passwort nicht ausgeschlossen werden kann.

Außerdem können Textnachrichten, Internet-Telefonie, Videokonferenzen oder ähnliches abgefangen werden. Auch auf Mikrofone und Kameras, die an den Rechner angeschlossen sind, kann zugegriffen werden, um so die Umgebung des Rechners zu überwachen.

Es ist nicht auszuschließen, dass die Zielperson den „Trojaner“ entdeckt, wenn ihr zum Beispiel die Menge der übertragenen Daten auffällt. Dies kann entweder zur Folge haben, dass der Nutzer die Spionagesoftware entfernt und so die Online-Durchsuchung vorzeitig beendet oder er übermittelt nur noch unverdächtiges Datenmaterial, um die Ermittler zu täuschen. Möglich wäre sogar, den Rechner der Ermittler zu infiltrieren, auszuspionieren und zu manipulieren.[2]

Da eine Online-Durchsuchung wohl nur für einen bestimmten Zeitraum zugelassen würde, ist auch eine Funktion zur Beendigung der Maßnahme vorzusehen. Dies ist der vierte Schritt. Auch für die Fälle, in denen der

---

[1] Fox, DuD 2007, 827, 830.
[2] Hansen/Pfitzmann, DRiZ 2007, 225, 228.

Verdacht gegen die Zielperson entkräftet wird, muss das „Trojanische Pferd“ jederzeit deaktivierbar sein.[1]

Aus technischer Sicht ist nie auszuschließen, dass ein „Trojaner“ Fehler enthält. Außer bei einer direkten Installation ist auch immer zu befürchten, dass Unbeteiligte von der Maßnahme betroffen sind. Bei Entdeckung des „Trojanischen Pferdes“ ist ein „Gegenangriff“ zu befürchten. Zudem sind die gewonnenen Daten nicht so verlässlich, wie die von einem sichergestellten Rechner gewonnenen Daten, da technisch nicht nachzuweisen ist, dass die Ermittler die echten Daten erhalten (sei es durch Manipulation der Zielperson oder durch Dritte).[2]

4.5.2 Bewertung

Hier wird wieder das bereits bekannte Spannungsverhältnis deutlich. Einerseits besteht für den Staat die Pflicht, die Grundrechte seiner Bürger und allgemeine Rechtsgüter zu schützen. Andererseits haben die Bürger aber auch Freiheitsgrundrechte, die sie vor dem Staat schützen sollen. In einem Rechtsstaat muss darauf geachtet werden, dass die staatliche Macht begrenzt bleibt. Daher bedürfen alle Grundrechtseingriffe einer besonderen Rechtfertigung, auch wenn sie ihrerseits dem Schutz von Grundrechten dienen. Stehen der Schutz durch den Staat und der Schutz vor dem Staat in einem Konflikt, so hat der Gesetzgeber eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen. Kritiker, die äußern, dass „wenn ein moderner Rechtsstaat gegen kriminelle Machenschaften vorgehen will, dann muss endlich Schluss sein mit dem Wenn und Aber“[3], haben das Prinzip eines Rechtsstaats nicht verstanden.

---

[1] Hansen/Pfitzmann, DRiZ 2007, 225, 228.
[2] Hansen/Pfitzmann, DRiZ 2007, 225, 228.
[3] zit. nach Hunsicker, Kriminalistik 2007, 187, 188.

Der Hinweis auf ein aktuelles, konkretes Risiko setzt sich meist gegenüber einem abstrakten, langfristigen Risiko durch. So können Bedenken aufgrund von immer wieder neuen, zusätzlichen Ermächtigungen für staatliche Freiheitseingriffe leicht vergessen werden, wenn auf drohende terroristische Anschläge verwiesen wird. Um trotzdem in gewissem Maße zum Schutz der Grundrechte beizutragen, müssten die beiden wichtigen Datenschutzgrundsätze Zweckbindung und Datensparsamkeit stärker verankert werden. Durch eine nähere Definition der Eingriffsbefugnisse, auch in Bezug auf die anzuwendende Technik, wäre eine neue Entscheidung vorprogrammiert, sofern durch technischen Fortschritt weitergehende Maßnahmen möglich geworden sind.[1] All dies muss bedacht werden, wenn über eine Ermächtigungsgrundlage oder gar eine Änderung des Grundgesetzes nachgedacht wird.

4.5.2.1 Ermächtigungsgrundlage

Wie bereits erwähnt, lehnte der BGH die Anwendung der §§ 102 ff. StPO ab. Denn die heimliche Online-Durchsuchung sei, im Gegensatz zu der in den oben genannten Paragraphen geregelten offenen Durchsuchung, eine Zwangsmaßnahme mit neuem, eigenständigem Charakter, da die Eingriffsintensität bei dieser viel höher liege.[2] Auch andere Eingriffsnormen sind nicht einschlägig.[3]

4.5.2.2 Verfassungsrechtliche Zulässigkeit

Artikel 1 Abs. 1 GG gewährt einen „absolut geschützten Kernbereich privater Lebensgestaltung“ (Intimsphäre).[4] In diesem findet keine Abwägung zwischen den Grundrechten des Einzelnen und den öffentlichen Gefahrenabwehr- und Strafverfolgungsinteressen statt.[5] Die Überwachung muss unterbleiben, sobald Ansatzpunkte für eine

---

[1] Roßnagel, DRiZ 2007, 229 f.
[2] BGH, BGHSt 51, 211, 215.
[3] Hornung, DuD 2007, 575, 576.
[4] BVerfG, BVerfGE 109, 279, 313.
[5] Kutscha, NJW 2005, 20, 21.

Verletzung der Menschenwürde bestehen.[1] Werden solche Anhaltspunkte bekannt, ist eine bereits bestehende Überwachung sofort abzubrechen. Bereits erhobene Daten sind sofort zu löschen, da sie nicht mehr verwendet werden dürfen. Es sind ausreichende Schutzvorkehrungen zur Vermeidung von Grundrechtsverletzungen zu treffen.[2] Die Beachtung des Kernbereichsschutzes dürfte in der Praxis einige Schwierigkeiten bereiten. Denn im Regelfall kann erst nach Kenntnisnahme des Inhalts der gespeicherten Daten beurteilt werden, ob sie zum Kernbereich gehören. Das Bundesverfassungsgericht hat jedoch ausdrücklich festgestellt, dass es unzulässig ist, in den Kernbereich einzugreifen, um festzustellen, ob er betroffen ist.[3] Für dieses Problem ist bislang keine praktikable Lösung erkennbar.[4] Sollte es nicht möglich sein, die Online-Durchsuchung konform zum Kernbereichsschutz durchzuführen, wäre die Maßnahme insgesamt unzulässig.[5]

Artikel 13 Abs. 1 GG schützt die Unverletzlichkeit der Wohnung. Gewährt wird hier der Schutz der räumlichen Privatsphäre. Dieser Schutz wirkt auch gegenüber einer Überwachung der Wohnung durch technische Hilfsmittel von außerhalb.[6] Der Schutz von Artikel 13 Abs. 1 GG wird nicht dadurch aufgehoben, dass der Nutzer des Systems dieses mit dem Internet verbindet. Dies ist, wie bereits dargelegt, eine unerlässliche Voraussetzung für die Online-Durchsuchung. Sobald sich das infiltrierte System in der Wohnung befindet, ist Artikel 13 Abs. 1 GG anwendbar.[7] Eine gesetzliche Ermächtigungsgrundlage für die Online-Durchsuchung muss sich daher an Artikel 13 GG messen lassen. Da in diesem kein solcher Eingriff vorgesehen ist, wäre eine Änderung des Grundgesetzes

---

[1] BVerfG, BVerfGE 109, 279, 318.
[2] Roßnagel, DRiZ 2007, 229, 230.
[3] BVerfG, BVerfGE 109, 279, 323.
[4] Kutscha, NJW 2007, 1169, 1171.
[5] Hornung, DuD 2007, 575, 577.
[6] BVerfG, BVerfGE 109, 279, 309.
[7] Hornung, DuD 2007, 575, 577 f.

erforderlich. Ob der Anlass diese tief greifende Maßnahme rechtfertigt, ist zu bezweifeln.[1]

Die Online-Durchsuchung im Ermittlungsverfahren würde sich gegen einen konkreten Beschuldigten richten. Die erhobenen Daten sind stets personenbezogen und betreffen daher sein Grundrecht auf informationelle Selbstbestimmung. Die Einschränkung der Befugnis des Einzelnen, selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen[2], ist nur im überwiegenden Allgemeininteresse zulässig und muss dann dem Verhältnismäßigkeitsprinzip entsprechen. Der verfolgte Zweck, nämlich die wirksame Strafverfolgung und Verbrechensbekämpfung ist durchaus legitim.
Zur Eignung der Maßnahme lässt sich mangels Informationen und Erfolgsbeispielen nicht viel sagen. Da der Gesetzgeber insoweit einen Entscheidungsspielraum hat, wird er die Geeignetheit wohl bejahen. Er muss jedoch die Entwicklung ständig beobachten, um zu prüfen, ob das Ermittlungsinstrument tatsächlich geeignet ist, das verfolgte Ziel zu erreichen.[3]
Die Maßnahme ist erforderlich, sofern kein milderes Mittel existiert, welches ebenso zielführend ist. Laut BGH ist die offene Durchsuchung des Systems im Rahmen einer Wohnungsdurchsuchung das mildere Mittel.[4] Daher ist die Online-Durchsuchung verfassungsrechtlich nur zulässig, wenn die herkömmliche Durchsuchung mit Beschlagnahme des Computers den Erfolg der Maßnahme vereiteln würde. Dies wird in den meisten Fällen nicht zutreffen.[5] Einen Nachteil hat die herkömmliche Durchsuchung jedoch. So genannte flüchtige Inhalte, wie zum Beispiel anonyme Eintragungen in einem Online-Forum, sind in der Regel nicht rekonstruierbar, wenn auf dem System keine Kopien gespeichert wurden. Ebenso können Daten, die vollständig und nicht revidierbar gelöscht

[1] Hornung, DuD 2007, 575, 578.
[2] BVerfG, BVerfGE 65, 1.
[3] BVerfG, BVerfGE 109, 279, 340.
[4] BGH, BGHSt 51, 211, 215.
[5] Hornung, DuD 2007, 575, 579.

wurden, nicht rekonstruiert werden. Verschlüsselte Daten können nur mit Hilfe eines Passworts entschlüsselt und gelesen werden. Liegt dieses Passwort nicht vor, ist eine Rekonstruktion der Daten in der Regel nicht möglich.[1] Solche Daten könnten bei einer Online-Durchsuchung erfasst werden.

Um zu entscheiden, ob der Eingriff angemessen ist, sind den Vorteilen der Online-Durchsuchung die verursachten Grundrechtsbeeinträchtigungen gegenüber zu stellen. Maßgeblich hierbei ist die Intensität des Eingriffs. Bedenkt man die Sensibilität und den Umfang der Daten, sowie die Rechtsschutzdefizite durch die Heimlichkeit der Maßnahme, wie auch die Tatsache, dass eine Beeinträchtigung Dritter nicht ausgeschlossen werden kann, so ist die Eingriffsintensität als hoch zu beurteilen.[2] Außerdem besteht die Gefahr, dass die generelle Online-Sicherheit der Bürger und die Kommunikation der Gesellschaft insgesamt beeinträchtigt werden. Außerdem könnte die Vertrauenswürdigkeit der Computerbranche unterhöhlt werden. Da nämlich für die Infiltration eines „Trojanischen Pferdes“ eine Sicherheitslücke erforderlich ist, besteht die Gefahr, dass diese nicht mehr publik gemacht werden, um zu verhindern, dass die Bürger sich schützen und die Sicherheitslücken schließen können. Objektiv zumutbar und damit verhältnismäßig ist die Online-Durchsuchung nur dann, wenn sie ausschließlich der Verfolgung sehr schwerer Straftaten dient, wenn tatsächliche Anhaltspunkte für die Wahrscheinlichkeit eines Beitrags zum Ermittlungserfolg bestehen und wenn andere Maßnahmen aussichtslos sind.[3]

Sollte es Regelungen zur Online-Durchsuchung geben, müssten zusätzlich einige rechtsstaatliche Vorgaben beachtet werden. Zur Durchführung wäre eine richterliche Anordnung nötig. Die Maßnahme wäre zeitlich zu begrenzen. Die Daten dürften nur für das laufende Verfahren verwendet werden. Außerdem müssten die Beschuldigten nach Abschluss der Durchsuchungsmaßnahme benachrichtigt werden.

---

[1] Fox, DuD 2007, 827, 828.
[2] Hornung, DuD 2007, 575, 579.
[3] Hornung, DuD 2007, 575, 579 f.

Da jedoch eine einfachgesetzliche Regelung aufgrund des Artikels 13 GG nicht möglich ist und für eine Verfassungsänderung eine praktikable Lösung für den Schutz des Kernbereichs fehlt, sollte von diesem Vorhaben zumindest so lange abgesehen werden, bis die Eignung und Notwendigkeit der Online-Durchsuchung viel deutlicher gemacht werden kann, als bisher.[1]

5 Fazit

Das Ziel dieser Arbeit war es, bestehende Konflikte zwischen Datenschutz und den neu eingeführten Maßnahmen der Terrorismusbekämpfung darzulegen. Abschließend ist daher die eingangs gestellte Frage zu beantworten, ob man sich nun zwischen dem Schutz der personenbezogenen Daten und einer wirksamen Sicherheitsgesetzgebung im Kampf gegen den Terrorismus entscheiden muss.

Der Staat und mit ihm die Sicherheitsbehörden haben ein berechtigtes Interesse daran, sich ihre Arbeit in Bezug auf die Terrorismusbekämpfung so einfach wie möglich zu machen. Verständlich sind daher die Forderungen nach einem Abbau des Datenschutzes. Hier könnte erneut das eingangs genannte Zitat angeführt werden: „Wer nichts zu verbergen hat, benötigt keinen Datenschutz!“ Durch Offenlegung ihrer Daten könnten Bürger, die sich nichts haben zuschulden kommen lassen, ihre Unschuld beweisen. Dadurch würde jedoch ein wichtiger Pfeiler unseres Rechtsstaats, die Unschuldsvermutung, beseitigt.

Nach einem Bericht, den eine Untersuchungskommission im Sommer 2004 dem US-Kongress vorgelegt hat, gab es schon vor dem 11. September 2001 mehrere Möglichkeiten, die Anschlagspläne aufzudecken

[1] Hornung, DuD 2007, 575, 580.

und zu vereiteln. Bedeutsame Informationen über die Attentäter und ihre Aktivitäten waren bei verschiedenen Behörden bekannt, wurden jedoch nicht als relevant eingestuft.[1] Dies bedeutet, dass schon vor den Anschlägen ausreichende Eingriffsbefugnisse für die Sicherheitsbehörden vorhanden waren, aber die Informationen nicht richtig gedeutet wurden. Auch in Deutschland gab es teilweise, wie oben schon erwähnt, Vollzugsdefizite bei der Umsetzung bestehender Regelungen. Weitere Befugnisse für die Sicherheitsbehörden würden demnach zwar helfen, noch mehr Informationen zu sammeln, jedoch werden die anwachsenden Datenmengen nicht dazu beitragen können, dass aus den vorhandenen Erkenntnissen die richtigen Schlüsse für eine wirksame Verbrechensbekämpfung gezogen werden.
Daher darf der Staat nicht in einen gesetzgeberischen Aktionismus verfallen und neue Regelungen schaffen, ohne zuvor deren Wirksamkeit präzise überprüft zu haben. Denn die Gefahr ist groß, dass sich die Demokratie in Richtung eines Überwachungsstaats entwickelt.
Möglicherweise ist es genau dies, nämlich die Preisgabe verfassungsrechtlich garantierter Freiheitssicherung, was Terrorismus bezwecken soll. Um dem nicht zu entsprechen, muss sachlich und bedacht innerhalb der freiheitlichen Ordnung vorgegangen werden. Dabei ist auch immer zu bedenken, dass es eine hundertprozentige Sicherheit nicht gibt. Um den Terrorismus wirksam zu bekämpfen, darf man sich nicht nur auf eine Ausweitung der Sicherheitsgesetzgebung beschränken. Denn diese greift meist erst nach einem erfolgten Anschlag ein. Statt dessen sind die Ursachen zu erkunden und dem Terrorismus auf politischer und gesellschaftlicher Ebene wirksam vorzubeugen.

Es wäre daher verfehlt zu sagen, dass der Datenschutz den Kampf gegen den Terrorismus behindert. Er ruft statt dessen ins Bewusstsein, dass es um den Erhalt des demokratischen Rechtsstaates geht, zu dem auch das

[1] Schaar, 137.

Recht auf informationelle Selbstbestimmung gehört, und er bewahrt die Bürger vor unkontrollierten Eingriffen in ihre Grundrechte.
Hierzu sind Personen notwendig, die die Beachtung des Datenschutzes anmahnen und dies in die öffentliche Diskussion einbringen. Dies geschieht bereits unter anderem durch die Beauftragten für den Datenschutz. Auch das Bundesverfassungsgericht hat in der Vergangenheit nicht nur einmal eindeutig Stellung für den Datenschutz bezogen. In seinem Urteil aus dem Jahr 2004 zum so genannten „Großen Lauschangriff“ stellte es die Maßstäbe klar, die gelten, wenn der Staat in den Kernbereich der privaten Lebensgestaltung überwachend eingreifen will.
Für die Zukunft lässt dies hoffen, dass nicht alle gewünschten Maßnahmen ohne Weiteres umgesetzt werden können, weil Organe vorgesehen sind und bestehen, die die berechtigten Interessen der Bürger in Bezug auf ihr privates Leben und ihre Daten im Blick haben und die entsprechenden gesetzlichen Bestimmungen zur Anwendung bringen.

Abschließend kann man sagen, dass eine Entscheidung „entweder oder“ zwischen Datenschutz und Sicherheit nicht getroffen werden kann und muss, sondern dass beides möglich und sogar notwendig ist. Datenschutz und Sicherheit stehen in einer sich immer wieder verändernden Balance. Wird der Sicherheit der Vorzug gegeben, muss der Eingriff gerechtfertigt sein. Die Regelungen des Datenschutzes zeigen dabei auf, wo sinnvoll agiert werden kann, ohne unverhältnismäßig in Grundrechte einzugreifen.

Anlage 1

Bekämpfung des Terrorismus

Der internationale Terrorismus hat sich mit den Anschlägen des 11. September 2001 zu einer weltweiten Bedrohung entwickelt. Das Ausmaß der Gewaltbereitschaft, die logistische Vernetzung und die langfristig angelegte und grenzüberschreitende Vorgehensweise der Täter haben die Gefährdung deutlich vor Augen geführt.

Die Bundesregierung hat die Sicherheitsstrukturen unseres Landes mit einer Reihe umfangreicher gesetzlicher und administrativer Maßnahmen gezielt ausgebaut und der neuen Bedrohungslage angepasst. Mit den Sicherheitspaketen I und II wurde unter anderem die Aufklärungsarbeit im Vorfeld terroristischer Aktivitäten erheblich verbessert. So könnten beispielsweise wichtige Erkenntnisse über die Reisebewegungen, den Verlauf der Finanzströme oder die Vorgehensweisen beim Identitätswechsel Verdächtiger gewonnen werden.

Die Bekämpfung des islamistischen Terrorismus ist eine erstrangige Aufgabe für die Sicherheitsbehörden. Möglichen Gefährdungen durch extremistische Gruppierungen von rechts und links gilt dabei weiterhin die volle Wachsamkeit.

Im Vordergrund steht jedoch zweifellos die unverändert anhaltende Bedrohung durch den islamistischen Terrorismus. Die Sicherheitsbehörden des Bundes gehen seit geraumer Zeit davon aus, daß in Deutschland noch unbekannte islamistische Zellen existieren können, die in grenzüberschreitende funktionsfähige Strukturen eingebunden sind.

Fünf wichtige Ziel-Dimensionen bestimmen die Anti-Terror-Politik:

1. Terroristische Strukturen durch hohen Fahndungs- und Ermittlungsdruck zerstören

Um die Bekämpfung des Terrorismus nachhaltig zu verbessern, wurden mit dem zum 1. Januar 2002 in Kraft getretenen Terrorismusbekämpfungsgesetz die Kompetenzen des Bundeskriminalamtes und des Bundesamtes für Verfassungsschutz zur Informationsgewinnung und zum Informationsaustausch erweitert und ausländer- und vereinsrechtliche Regelungen geändert.

Zahlreiche strafrechtliche Ermittlungsverfahren wurden in Gang gesetzt und führten auch bereits zu hohen Schuldsprüchen. Seit dem 11. September 2001 wurden vier bedeutende Strafverfahren durch Verurteilungen abgeschlossen, zwei weitere werden derzeit vor Gericht verhandelt.

2. Terrorismus bereits im Vorfeld abzuwehren

Deutschland tritt dem Terrorismus energisch und frühzeitig entgegen. Extremismus muss bereits im Vorfeld entschieden der Boden entzogen werden. Gegen die islamistisch-extremistischen Organisationen "Kalifatstaat", mit weiteren Teilorganisationen (am 12. Dezember 2001), "Al-Aqsa e.V." (am 5. August 2002) und "Hizb-ut Tahrir" (am 15. Januar 2003)), "Yeni Akit GmbH" (am 25. Februar 2005) sowie "YATIM Kinderhilfe e.V." (am 5. September 2005), eine Nachfolgeorganisation von "Al-Aqusa e.V." (am 05. September 2005), wurden daher Verbote verhängt.

Um Terroristen möglichst frühzeitig an der Einreise nach Deutschland hindern zu können, ist es notwendig, die Identitätsüberprüfung im Reiseverkehr und die Fälschungssicherheit von Ausweisdokumenten zu verbessern. Die Bundesregierung treibt daher den Einsatz biometrischer Merkmale - Fingerabdrücke, Lichtbilder oder Irisfotos - in drei Bereichen voran:

- bei der Kontrolle der nach Deutschland einreisenden Personen,
- bei Visa und Aufenthaltstiteln und
- bei Pässen und Personalausweisen.

3. Internationale Zusammenarbeit weiter auszubauen

Die Vielzahl der internationalen Anknüpfungspunkte des terroristischen Netzwerkes macht es unabdingbar, den eingeschlagenen Weg konsequenter internationaler Zusammenarbeit fortzusetzen und weiter auszubauen. Dem transnational handelnden islamistischen Terrorismus ist wirksam nur in enger internationaler Kooperation beizukommen. Gemeinsam wurden in den Vereinten Nationen, der G 8 und der EU bereits zahlreiche Vereinbarungen erreicht. Deutschland hat weitere Initiativen in die EU eingebracht, die auf eine Verbesserung des Informationsaustausches, der Identitätssicherung von visumspflichtigen Ausländern sowie der Fahndung nach Terroristen abzielen.

4. Bevölkerung schützen, vorsorgen und die Verwundbarkeit unseres Landes reduzieren

Um Anschläge in Deutschland zu verhindern, werden die Sicherheitsvorkehrungen regelmäßig untersucht und der aktuellen Bedrohungslage angepasst. Insbesondere durch eine Überprüfung der Infrastruktursysteme sind, beispielsweise im Luftverkehr, deutliche Sicherheitsgewinne erzielt worden. Die erforderlichen Maßnahmen zur Erhöhung etwa der Luftsicherheit wurden mit höchster Priorität eingeleitet und umgesetzt: zum Beispiel intensivierte Personen- und Gepäckkontrollen auf Flughäfen oder der Einsatz bewaffneter Flugbegleiter der Bundespolizei in Flugzeugen.

5. Ursachen des Terrorismus beseitigen

Um den Terrorismus auch in seinen instabilen Herkunftsregionen wirksam zurückdrängen, trägt die Bundesregierung zu den Einsätzen der internationalen Gemeinschaft bei. Deutschland beteiligt sich an der Operation "Enduring Freedom" am Horn von Afrika, im Golf von Oman und im Rahmen der Anti-Terror-Koalition bei der Bekämpfung des Terrornetzwerks in Afghanistan. Unser Land zeigt großes personelles und materielles Engagement in der internationalen Schutztruppe ISAF für die dauerhafte Befriedung Afghanistans und die Konsolidierung der Zivilgesellschaft. Das Bundesinnenministerium nimmt mit der Hilfe beim Aufbau der Polizei in Afghanistan aktiv an diesem Prozess teil.

Anlage 2

Gesetzgebung zur Terrorismusbekämpfung

Seit den Anschlägen in den USA vom 11. September 2001 hat der Gesetzgeber des Bundes zahlreiche Bestimmungen erlassen, die der Verbesserung des Kampfes gegen den internationalen Terrorismus dienen. Ein Teil dieser Regelungen wurde in Gesetzgebungsvorhaben integriert, die hauptsächlich andere Ziele betrafen. Ein bedeutender Teil dieser Bestimmungen ist aber in Gesetzen enthalten, die vorrangig und gezielt der Terrorismusbekämpfung dienen, nämlich dem **Terrorismusbekämpfungsgesetz (TBG)** und dem **Terrorismusbekämpfungsergänzungsgesetz (TBEG)**. Bei diesen Gesetzen handelt es sich um so genannte Mantelgesetze. Durch sie wurden keine neuen Gesetze geschaffen, sondern Änderungen an bestehenden Gesetzen vorgenommen. Zur Information über den aktuellen Stand der Gesetzgebung empfiehlt es sich daher, nicht das TBG oder das TBEG mit ihren Änderungsbefehlen zu studieren, sondern unmittelbar die aktuellen Gesetzestexte der jeweils geänderten Gesetze heranzuziehen. Die durch das TBG und das TBEG bewirkten Änderungen wurden in die Texte der geänderten Vorschriften eingearbeitet, die in der elektronischen Dokumentation des Bundesrechts des Bundesministeriums der Justiz unter http://www.gesetze-im-internet.de kostenfrei abrufbar sind.

Die folgende Übersicht zeigt die Änderungen auf, die das TBG und das TBEG gegenüber dem jeweils vorherigen Rechtszustand bewirkt haben.

1. Terrorismusbekämpfungsgesetz

Mit dem zum 1. Januar 2002 in Kraft getretenen Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz; kurz TBG) wurden zahlreiche Sicherheitsgesetze der neuen Bedrohungslage angepasst. Das Bundesverfassungsschutzgesetz, das MAD-Gesetz, das BND-Gesetz, das Bundespolizeigesetz, das Bundeskriminalamtgesetz sowie das inzwischen, zum 1. Januar 2005, durch das Aufenthaltsgesetz abgelöste damalige Ausländergesetz und andere ausländerrechtliche Vorschriften wurden geändert, um

- den Sicherheitsbehörden die nötigen gesetzlichen Kompetenzen zu geben,
- den erforderlichen Datenaustausch zwischen den Behörden zu verbessern,
- bereits die Einreise terroristischer Straftäter nach Deutschland zu verhindern,
- identitätssichernde Maßnahmen im Visumverfahren zu verbessern,
- den Einsatz bewaffneter Flugbegleiter der Bundespolizei auf deutschen Luftfahrzeugen zu ermöglichen,
- Grenzkontrollmöglichkeiten zu verbessern und
- bereits eingereiste Extremisten besser zu erkennen.

Zudem wurden das Sicherheitsüberprüfungsgesetz, das Passgesetz, das Gesetz über Personalausweise, das Vereinsgesetz, das Luftverkehrsgesetz, das Bundeszentralregistergesetz, das Zehnte Buch des Sozialgesetzbuchs und das Energiesicherungsgesetz wurden geändert, um

- Sicherheitsüberprüfungen für Mitarbeiter in lebens- oder verteidigungswichtigen Einrichtungen zu ermöglichen,
- Rechtsgrundlagen für die Aufnahme biometrischer Merkmale in Pässe und Personalausweise zu schaffen,
- den Gebrauch von Schusswaffen in zivilen Luftfahrtzeugen Polizeivollzugsbeamten vorzubehalten,
- Aktivitäten extremistischer Ausländervereine in Deutschland rascher unterbinden zu können,
- die Rasterfahndung durch die Einbeziehung von bestimmten Sozialdaten wirkungsvoller zu gestalten,
- die uneingeschränkte Energieversorgung sicherzustellen.

Zu den gesetzlichen Änderungen im Einzelnen:

Das **Bundesamt für Verfassungsschutz** hat das Recht erhalten, auch solche Bestrebungen zu beobachten, die sich gegen den Gedanken der Völkerverständigung oder gegen das friedliche Zusammenleben der Völker richten, da sie ein gefährlicher Nährboden für den wachsenden Terrorismus sind. Entsprechende Informationen können zur Feststellung von Tätern und Hintermännern führen. Zur Erforschung von Geldströmen und Kontobewegungen von Organisationen und Personen, die extremistischer Bestrebungen oder sicherheitsgefährdender bzw. geheimdienstlicher Tätigkeiten verdächtigt werden, hat das Bundesamt für Verfassungsschutz die Befugnis erhalten, Informationen bei Banken und Finanzunternehmen über Konten und Konteninhaber einzuholen. Ferner wurden Auskunftsbefugnisse gegenüber Postdienstleistern, Luftverkehrsunternehmen, Telekommunikations- und Teledienstleistern eingeführt. Die Befugniserweiterungen stehen dabei unter der strikten rechtsstaatlichen Kontrolle unabhängiger Gremien. Einige dieser Befugnisse haben auch MAD und BND erhalten.

Die originären Ermittlungskompetenzen des **Bundeskriminalamtes** wurden erweitert. So hat das Bundeskriminalamt die originäre Ermittlungskompetenz für bestimmte Computersabotage-Straftaten erhalten, wenn diese Taten zu erheblichen Auswirkungen auf die innere oder äußere Sicherheit führen oder sich gegen Stellen richten, deren Störung für große Bevölkerungsgruppen kritische Folgen haben würde. Das Bundeskriminalamt wurde auch in die Lage versetzt, auf Grund eines Anfangsverdachts unmittelbar Ermittlungen zu führen, ohne dazu zunächst beauftragt oder ersucht worden zu sein. Zudem wurde die Zentralstellenkompetenz des BKA gestärkt, und zwar ohne - wie nach altem Recht - vorher zeitaufwändig klären zu müssen, ob die Polizeien des Bundes oder der Länder über die Informationen verfügen.

Im **Bundespolizeigesetz** wurde zugunsten des Einsatzes von Sicherheitskräften der Bundespolizei an Bord von deutschen Luftfahrzeugen (Flugsicherheitsbegleiter) eine Klarstellung vorgenommen. Darüber hinaus erweiterte das Gesetz die Befugnis der Bundespolizei, im Rahmen seiner räumlichen und sachlichen Zuständigkeit Personen nicht nur anhalten und befragen, sondern auch die mitgeführten Ausweispapiere überprüfen zu können.

Im **Aufenthaltsrecht** wurden Bestimmungen vorgesehen, die verhindern, dass Personen Visa oder Aufenthaltsgenehmigungen erhalten, die die freiheitliche demokratische Grundordnung oder die Sicherheit der Bundesrepublik Deutschland gefährden, sich bei der Verfolgung politischer Ziele an Gewalttätigkeiten beteiligen, öffentlich zur Gewaltanwendung aufrufen oder einer Vereinigung angehören, die den internationalen Terrorismus unterstützt. Ihnen sind Einreise und Aufenthalt in Deutschland untersagt. Darüber hinaus wurde die Grundlage für eine Intensivierung der Zusammenarbeit der Auslandsvertretungen mit den Sicherheitsbehörden geschaffen. Die Möglichkeiten der Identitätssicherung, insbesondere von Auslandsvertretungen im Visumverfahren, wurden erweitert. Zudem wurde die Fälschungssicherheit von Ausweispapieren und aufenthaltsrechtlichen Dokumenten erhöht. Die durch das TBG geschaffenen Bestimmungen im damaligen Ausländergesetz wurden im später verabschiedeten Aufenthaltsgesetz sinngemäß übernommen.

Im **Asylverfahrensgesetz** wurde eine gesetzliche Grundlage für eine Sprachaufzeichnung geschaffen, anhand derer eine identitätssichernde Sprachanalyse zur Bestimmung der Herkunftsregion erfolgen kann. Auf die Erhebung muss der Ausländer vorher hingewiesen werden. Die Aufzeichnung erfolgt außerhalb der förmlichen Asylanhörung. Fingerabdrücke und andere im Zusammenhang mit Asylverfahren gewonnene identitätssichernde Unterlagen werden 10 Jahre ab Unanfechtbarkeit der Asylentscheidung aufbewahrt. Ebenso können die Fingerabdrücke von Asylbewerbern seit der Gesetzesänderung automatisch mit dem polizeilichen Tatortspurenbestand des Bundeskriminalamtes abgeglichen werden.

Schließlich wurde die Erkenntnisgewinnung aus dem Ausländerzentralregister durch wichtige Änderungen des **Ausländerzentralregistergesetzes** verbessert. Die Visadatei, in der derzeit grundsätzlich nur Daten über Visaanträge gespeichert werden, wurde zu einer Visaentscheidungsdatei ausgebaut, um eine verbesserte Kontrolle des einreisenden Verkehrs zu gewährleisten. Der Zugriff für Polizeibehörden z.B. im Rahmen von Personenkontrollen wurde verbessert, damit sie sofort feststellen können, ob sich ein Ausländer legal in Deutschland aufhält. Die Möglichkeit, Gruppenauskünfte (Auskünfte über Personen, die bestimmte einzelne Merkmale erfüllen, ohne dass alle Personalien bekannt sind) einzuholen, wurden ausgedehnt; zudem wurde geregelt, dass Daten für die jeweils berechtigten Behörden „online" und nicht nur durch Schreiben an das Zentralregister zugänglich sind.

Weitere Änderungen sah das Gesetz für das **Sicherheitsüberprüfungsgesetz**, das Luftverkehrsgesetz, das Bundeszentralregistergesetz, das Passgesetz, das Gesetz über Personalausweise, das Vereinsgesetz, das Zehnte Buch Sozialgesetzbuch und das Energiesicherungsgesetz vor. Im Sicherheitsüberprüfungsgesetz wurden z.B. erstmals Vorschriften für Maßnahmen des vorbeugenden personellen Sabotageschutzes geschaffen. Personen, die in lebens- oder verteidigungswichtigen Einrichtungen tätig sind oder werden sollen, werden seit Inkrafttreten des Gesetzes sicherheitsüberprüft.

Mit der Änderung des **Luftverkehrsgesetzes** erfolgte eine Klarstellung, dass der Gebrauch einer Schusswaffe an Bord eines zivilen Luftfahrzeuges Polizeivollzugsbeamten, insbesondere der Bundespolizei im Rahmen ihrer Sicherheitsbegleitung, vorbehalten ist. Weitere Regelungen betrafen Zuverlässigkeitsüberprüfungen des bei Flugplatz- und Luftfahrtunternehmen in sicherheitsrelevanten Bereichen beschäftigten Personals; die Überprüfung wurde auf das beim Flugsicherungsunternehmen beschäftigte Personal und andere Personen mit sicherheitssensiblen Aufgaben ausgedehnt. Die Folgeänderung des **Bundeszentralregistergesetzes** ermöglicht den Luftfahrtbehörden die Einholung einer unbeschränkten Auskunft über einen Personenkreis, der gegenüber der früheren Rechtslage erweitert wurde.

Im **Pass- und Personalausweisrecht** wurde eine Grundlage für die computergestützte Identifizierung von Personen auf der Grundlage der Ausweisdokumente geschaffen, um zu verhindern, dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen. Neben dem Lichtbild und der Unterschrift darf ein weiteres biometrisches Merkmal - auch in verschlüsselter Form - in den Pass und den Personalausweis aufgenommen werden. Die näheren Einzelheiten wurden inzwischen auch im Recht der Europäischen Union festgelegt; bei dem Merkmal handelt es sich um den Fingerabdruck.

Nach der Streichung des "Religionsprivilegs" ergänzen Änderungen des **Vereinsgesetzes** die staatlichen Handlungsoptionen zur Bekämpfung extremistischer Vereinigungen mit Auslandsbezug. So konnte mit der Neufassung und Ausweitung der Vereinsverbotsgründe für Ausländervereine und ausländische Vereine z.B. verhindert werden, dass gewalttätige oder terroristische Organisationen von Ausländervereinen in Deutschland unterstützt werden. Das Verbot der öffentlichen Verwendung von Kennzeichen verbotener Vereine wurde zudem effektiver gestaltet.

2. Evaluierung des TBG

Die Regelungen des TBG zum Bundesverfassungsschutzgesetz, dem BND-Gesetz, dem MAD-Gesetz, dem Sicherheitsüberprüfungsgesetz sowie dem § 7 Abs. 2 des BKA-Gesetzes wurden auf fünf Jahre befristet. Vor Ablauf dieser Frist wurde die Wirksamkeit der Regelungen evaluiert.

Der vom Bundeskabinett am 11. Mai 2005 beschlossene entsprechende Evaluierungsbericht ist in der öffentlichen Sitzung des Innenausschusses des Deutschen Bundestages am 1. Juni 2005 von allen Fraktionen positiv gewürdigt worden. Der Bericht kommt zu dem Ergebnis, dass es richtig war, die Befugnisse der Sicherheitsbehörden maßvoll zu erweitern. Sie sind gleichermaßen erfolgreich wie zurückhaltend und verantwortungsvoll genutzt worden.

Zum Download bzw. als Link stehen folgende Informationen zur Verfügung:

- Fakten zur Evaluierung des Terrorismusbekämpfungsgesetzes
- Bericht der Bundesregierung zur Evaluierung des Terrorismusbekämpfungsgesetzes

3. Terrorismusbekämpfungsergänzungsgesetz (TBEG)

Mit dem TBEG, das am 10. Januar 2007 im Bundesgesetzblatt verkündet worden ist, wurden die Schlussfolgerungen aus der Evaluierung umgesetzt. Die inzwischen bewährten Befugnisse der Sicherheitsbehörden wurden für weitere fünf Jahre befristet beibehalten und dabei zugleich praxisgerechter gestaltet und an aktuelle Erfordernisse der Terrorismusbekämpfung angepasst.

Eine wesentliche Neuerung ist nach dem TBEG, dass das Bundesamt für Verfassungsschutz seine bestehenden Auskunftsbefugnisse künftig auch zur Aufklärung bisher noch nicht erfasster verfassungsfeindlicher Bestrebungen einsetzen kann, wenn diese die Bereitschaft zur Anwendung von Gewalt fördern. Hierbei kann es sich genauso um Hetze rechtsextremistischer Organisationen wie um islamistische Hasspredigten handeln. Es kommt nicht mehr darauf an, ob ein Hassprediger gegen andere Völker oder aber gegen Ungläubige in Deutschland hetzt. Im Einzelnen sieht das TBEG darüber hinaus zum Beispiel vor, dass das Bundesamt für Verfassungsschutz leichter Auskünfte von Fluggesellschaften über Flugbuchungen verdächtiger Personen erhalten kann. Die Aufgaben des Bundesnachrichtendienstes werden nicht geändert.

Im Einzelnen wurden das Bundesverfassungsschutzgesetz, das MAD-Gesetz, das BND-Gesetz, das Artikel 10-Gesetz, das Vereinsgesetz, das Passgesetz, das Zollverwaltungsgesetz, das Straßenverkehrsgesetz, das Luftsicherheitsgesetz und die Sicherheitsüberprüfungsfeststellungsverordnung geändert.

Zum Download bzw. als Link stehen folgende Informationen zur Verfügung:

- Pressemitteilung vom 10. Januar 2007 - "Terrorismusbekämpfungsergänzungsgesetz tritt morgen in Kraft"
- Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes (Terrorismusbekämpfungsergänzungsgesetz)
- ausführliche Erläuterungen zu den einzelnen Befugnissen und Neuregelungen des TBEG

Anlage 3

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg

Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der "Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes" kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der "Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes" ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

Anlage 4

Cordelia Koch

Freiheitsbeschränkung in Raten?

Biometrische Merkmale und das Terrorismusbekämpfungsgesetz

HSFK-Report 5/2002

Hessische Stiftung Friedens- und Konfliktforschung

[...]

nicht der Fingerabdruck oder das Foto selbst wird dann mit einem gespeicherten Datensatz abgeglichen."[9]

Indem ein möglichst einzigartiges Körpermerkmal in einen Datensatz übersetzt wird, können die biometrischen Verfahren grundsätzlich also eine sehr viel spezifischere Identifikation einer Person ermöglichen, als dies durch die bisherige Praxis der Personenbeschreibung, der Nennung besonderer Kennzeichen, der Unterschrift und dem Foto möglich ist. Wenn auch Unterschrift und Foto biometrische Merkmale sind, erschweren aber Unterschriftsfälschung und Alterungsprozess die eindeutige Identifikation der Person. Von den bisher im Pass befindlichen biometrischen Merkmalen unterscheiden sich die des Artikel 7 TerrorbekG durch ihre vielseitige Verwendbarkeit. Sie ordnen sich ein in eine Reihe von Maßnahmen, die unter dem Thema „privacy" behandelt werden, wie zum Beispiel die Diskussion um Videokameras im öffentlichen Raum zur Kriminalitätsbekämpfung.[10] Die juristische Debatte darüber, ob der „Überwachungsstaat auf dem Vormarsch – der Rechtsstaat (hingegen) auf dem Rückzug"[11] ist, begann auch nicht erst mit den gesetzlichen Maßnahmen nach dem 11. September 2001.

Was rechtfertigt einen Report allein über ein paar Zeilen neues Gesetz? Warum all die Aufregung über biometrische Merkmale im Pass? Die Verknüpfung biometrischer Merkmale im Pass mit der Terrorismusbekämpfung ist geeignet, eine Grundregel unseres Rechtsstaats umzukehren. Dazu könnte es kommen, wenn statt der Unschuldsvermutung der Passinhaber gegen die Schuldvermutung des biometrischen Merkmals seine Unschuld beweisen muss.[12] Wenn nun die biometrischen Merkmale eine Schuldvermutung zu Ungunsten der Staatsbürger aufbauten, würde uns dies rechtstechnisch in das tiefe Mittelalter zurückwerfen. Daraus ergibt sich die Brisanz der Erfassung biometrischer Merkmale im Pass.[13] Deshalb muss nicht nur sorgsam überprüft werden, ob die Aufnahme biometrischer Merkmale in den Pass das von ihr anvisierte Sicherheitsziel erreicht. Darüber hinaus ist dem Zweck der biometrischen Merkmale und den durch sie eintretenden Freiheitsbegrenzungen allergrößte Aufmerksamkeit zu schenken. Damit ergibt sich die Problematik aus der Berechtigung des Sicherheitsziels auf der einen und der doppelten Frage nach der Sinnhaftigkeit der Maßnahme im Vergleich zum anvisierten Ziel und ihrer Verhältnismäßigkeit im Vergleich zur Freiheitsbeschränkung auf der anderen Seite.

9 Thomas Vacek/Sven Scheffler, Das gestohlene Gesicht, in: Die Zeit, Nr. 46/2001, www.zeit.de/2001/46/Wissen/200146_biometrie.html (10. April 2002).

10 Vgl. zu der umfassenden Problematik die Informationen der Nichtregierungsorganisation: Privacy International unter: www.privacyinternational.org oder auch: www.statewatch.org.

11 So der Titel eines Aufsatzes von Horst Hund in der Neuen Juristischen Wochenschrift, Nr. 34, 1992, S. 2118–2123.

12 So: Helmut Bäumler, Landesbeauftragter für Datenschutz, Interview in den Lübecker Nachrichten vom 20. Oktober 2001: www.rewt.hu-berlin.de/Datenschutz/DSB/SH/material/themen/presse/ln201001.htm (28.03.2002).

13 Wenn nachfolgend von der Problematik biometrischer Merkmale gesprochen wird, ist damit immer die Erfassung, nicht das objektiv existente biometrische Merkmal gemeint.

2. Sicherheit und Freiheit im demokratischen Verfassungsstaat

Das Dilemma zwischen Freiheitssicherung und Sicherheitsgewährleistung stellt sich nicht nur in diesem Fall. Es kennzeichnet den demokratischen Verfassungsstaat: Als Kernthemen sind Freiheit und Sicherheit seit Bodin, Hobbes, Montesquieu, Locke und der Erklärung der Menschen- und Bürgerrechte von 1789 nebeneinander und untrennbar mit dieser Organisation eines politischen Gemeinwesens verbunden. Das Verhältnis von Freiheit und Sicherheit ist dabei zwar immer eine politische Frage, die sich in Schlagworten wie „Freiheit durch Sicherheit", „Freiheit als Begrenzung der Sicherheit", „Sicherheit und Freiheit" ausdrücken lässt. Letztlich hängt aber die Entscheidung für den Vorrang der Sicherheit oder eine starke Gewichtung der Freiheit von der persönlichen Auffassung über den Staat und seine primären Aufgaben ab. Wer einen „starken" Staat befürwortet, legt großes Gewicht auf die Sicherheitskomponente, der Anhänger eines „liberalen" Staates will die Sicherheitskomponente eng definieren und misst der Beachtung von Freiheitsrechten größte Bedeutung zu. Man kann vielleicht soweit gehen, dass sich in der Gewichtung von Freiheit und Sicherheit auch die persönliche Vorstellung über die Beziehung zwischen Staat und Bürger widerspiegelt: tendenziell obrigkeitsstaatlichem Denken steht eine Vorstellung von der Autonomie der Bürger entgegen, die auf bisher erkämpfte Grundfreiheiten und Machtbegrenzungen aufbaut. Jedenfalls will der demokratische Verfassungsstaat beide Komponenten verwirklichen – keine von beiden darf ausschließlich zur Geltung gebracht werden, weil der totalitäre Staat beziehungsweise Willkür unter den Staatsbürgern die Folge wären. Freiheit und Sicherheit sind *beide* Grundvoraussetzungen und „Lebensgrundlage" der Demokratie, die auf der Selbstbestimmung der Bürger aufbaut. Selbstbestimmung kann aber wiederum nur in einem von Gewalt und Willkür freien Umfeld ausgeübt und verwirklicht werden.

Jede Sicherheitsmaßnahme tangiert und beschränkt notgedrungen die Freiheit der Bürger, während die Verwirklichung der maximalen Freiheit zu Einbussen auf dem Gebiet der Sicherheit führt: Wenn jeder tun und lassen kann, was er will, lebt niemand in Sicherheit, d. h. in dem sicheren Bewusstsein, dass bestimmte, an die anderen gerichtete Verhaltenserwartungen nicht enttäuscht werden. Dabei geht es nicht nur um das elementare Recht auf Leben, das an prominenter Stelle – in Artikel 2 Absatz 2 Satz 1 Grundgesetz – von unserer Verfassung garantiert wird. Sicherheit umfasst ebenso die Gewissheit, dass Verträge erfüllt, erlittene Schäden ausgeglichen und Straßenregeln befolgt werden, so dass unser tagtägliches Verhalten mit ihrer Gewährleistung verbunden ist. Ein so weit gefasster Sicherheitsbegriff kann deshalb nicht nur als Begrenzung der Freiheit verstanden werden. Sicherheit ist gleichzeitig auch Voraussetzung der Freiheit. Damit lassen sich in einem ersten Schritt (neben dem Argument des bestehenden Sicherheitsinteresses) Sicherheitsmaßnahmen *begründen*. In einem zweiten Schritt muss die jeweilige Sicherheitsmaßnahme allerdings daraufhin überprüft werden, ob sich ihre konkrete Ausgestaltung *rechtfertigen* lässt. An dieser Stelle muss die Kehrseite der Medaille, der für den Sicherheitserfolg zu entrichtende Preis der Freiheitsbeschränkung, in Rechnung gestellt werden, um die eigenständige und elementare Bedeutung von Freiheit in einer Demokratie zur Geltung zu

bringen. Die Abwägung zwischen Haben und Soll orientiert sich dabei an der Frage, wie das Sicherheitsplus im Blick auf das Freiheitsminus zu beurteilen ist.

Sicherheitsmaßnahmen können also in einer Demokratie weder allein an ihrem Erfolg gemessen, noch allein mit ihrem Langzeitziel, der „Freiheit in Sicherheit", begründet werden, wodurch das Verhältnis von Freiheit und Sicherheit damit einer schwierig zu leistenden Balance gleicht. In diesem Sinne stellt die Verwirklichung von Freiheit und Sicherheit eine Antinomie der Staatsform Demokratie dar: Beide stehen zwar in einem unauflösbaren Widerspruch zueinander, sind aber gerade in der Idee der Demokratie mitgedacht und sollen immer gleichzeitig verwirklicht sein. Die Frage, wie die Staatsorgane mit dieser Antinomie umgehen, ob sie in den staatlichen Entscheidungen die Balance halten oder auch nur anstreben, sagt aber nicht nur etwas darüber aus, wie es um die Demokratie steht. Es ist die Aufgabe der Gesetzgebungsorgane, die persönlichen Präferenzen der Staatsbürger zum Verhältnis von Freiheit und Sicherheit anlässlich einer bestimmten Maßnahme zu aggregieren. Idealiter sollte ein Konsens zwischen Staatsbürgern und Staatsorganen Ergebnis des Gesetzgebungsvorgangs sein. Wird dieser Konsens nicht gesucht oder zumindest dauerhaft nicht erreicht, ergeben sich Spannungen, die schlussendlich den Rechtsfrieden stören können.

Wie muss man sich ihr Verhältnis nun vorstellen? Das Verhältnis von Freiheit und Sicherheit ist kein allgemeingültiges, in dem Sinne, dass alle Mitglieder einer Gesellschaft hierüber einer Auffassung wären. Es ist darüber hinaus aber auch kein überzeitliches und unveränderliches. Eine Situation der Bedrohung, etwa durch Terrorakte, kann das Verhältnis zugunsten der Sicherheitsbelange verschieben und Eingriffe in Freiheitsbereiche rechtfertigen, die unter „normalen" Umständen nicht akzeptabel wären. Das Verhältnis von Freiheit und Sicherheit ist daher situationsbedingt anzupassen, was bedeutet, dass die anzustrebende „Balance" variiert. Die in dem Terrorismusbekämpfungsgesetz zusammengefassten Sicherheitsgesetze müssen in diesem Sinne als ein Versuch der situationsbedingten Ausbalancierung von Sicherheit und Freiheit aufgefasst werden. Das Gesetzespaket wurde jedoch gerade aufgrund der Vorverlegung staatlicher Aktivität zur Abwehr feindlicher Tendenzen in Rechtssphären, die in einem freien Staat durch Individualrechte gesichert sind, stark kritisiert.[14] Rechtsgrundsätze würden von den Staaten des Westens im Wettlauf geopfert zugunsten von Maßnahmen, die Kennzeichen einer Diktatur seien.[15] Der Geist der Gesetze sei verseucht von den Terroristen.[16] Wer diese Ansicht über das Terrorismusbekämpfungsgesetz vertritt, kam offensichtlich zu dem Schluss, dass die situationsbedingte Anpassung der Gesetze an die (veränderte) Sicherheitslage weit über das Ziel hinaus geschossen ist und es sich nicht um eine ausbalancierte Lösung des Sicherheitsproblems handelt.

14 Christoph Gusy bei der Sachverständigen-Anhörung im Innenausschuss des Bundestages, zitiert nach: Heribert Prantl, Der Terrorist als Gesetzgeber, in: Süddeutsche Zeitung vom 8./9. Dezember 2001, S. 13.

15 Aufgrund der Vorverlegung der Abwehrmaßnahmen.

16 So Heribert Prantl, Der Terrorist als Gesetzgeber, in: Süddeutsche Zeitung vom 8/9. Dezember 2001, S. 13.

Der Grund hierfür könnte darin liegen, dass ein Terrorakt zum Anlass genommen wurde für eine Veränderung der Sicherheitsgesetze. „Terror" impliziert Unberechenbarkeit und Unvorhersehbarkeit, so dass *Sicherheitsmaßnahmen* zur Verhinderung des Terrorismus sehr weitgehend sein müssen. Kann man indes überhaupt fordern, dass der Staat seine Bürger vor terroristischen Anschlägen zu schützen habe? Nur dann, wenn man diese Frage abstrakt beantwortet, ohne auf die Art und Weise, den Umfang und das Ziel des Schutzes einzugehen, fällt ihre Bejahung leicht.

Der Titel des „Sicherheitspakets II" lässt aber vermuten, dass alle enthaltenen Gesetzesänderungen auf die Verbesserung, gar Gewährleistung der Sicherheitslage im Hinblick auf den „internationalen Terrorismus" zielen. Hierzu werden ausschließlich sicherheitspolizeiliche Maßnahmen gewählt. In diesem Report wird nicht die Auffassung vertreten, dass der Staat *allein* durch Sicherheitsmaßnahmen absoluten Schutz vor terroristischen Anschlägen gewährleisten kann. Da nun aber das Gesetz den Zusammenhang zwischen seinem Inhalt und der Terrorismusbekämpfung herstellt, muss jede einzelne darin enthaltene Sicherheitsmaßnahme (neben ihrer Ausgestaltung der problematischen Balance von Sicherheit und Freiheit) geeignet sein, nicht nur irgendeinen Sicherheitserfolg zu erzielen, sondern gerade auch der Terrorismusbekämpfung zu dienen.

[...]

Anlage 5

Do 01. Nov 07

Weltinnenpolitik im 21. Jahrhundert - Neue Herausforderungen zwischen Stabilisierung und Prävention

Rede von Bundesinnenminister Dr. Wolfgang Schäuble beim 9. BND-Symposium "Zerfall der Ordnung – Crisis of Governance" am 1. November 2007 in Berlin

[...]

Politische Gestaltungsfähigkeit basiert mehr und mehr auf Information. Deswegen müssen wir mehr wissen. Das gilt für alle Bereiche, vor allem aber im Sicherheitsbereich. Das wichtigste Instrument im Kampf gegen den Terrorismus ist *intelligence*. Nur mit Informationen – auch nachrichtendienstlicher Informationen – haben wir eine Chance, Bedrohungen abzuwehren, bevor Schaden entstanden ist. Deswegen sind die Erlangung und Vernetzung von Informationen, effektive Ermittlungsarbeit und Kooperation der Behörden – national wie international – unverzichtbar. Je schneller und unkomplizierter wir grenzüberschreitend kommunizieren und Informationen austauschen, umso mehr Erfolg werden wir bei der Bekämpfung des internationalen Terrorismus haben.

Die globale Informationsgesellschaft ist eben auch die Basis des Verbrechens. Deswegen darf der demokratische Rechtsstaat – was die Nutzung und Kontrolle der Informationstechnologie betrifft – den Wettkampf mit den Gefährdern nicht verweigern. Wir müssen operativ auf der Höhe derjenigen bleiben, die unsere Sicherheit gefährden. Das heißt, wir müssen die technischen Mittel anwenden und kontrollieren, die Kriminelle und Terroristen im 21. Jahrhundert nutzen. Die Möglichkeit der klassischen Telekommunikationsüberwachung reicht hierfür nicht mehr aus.

Bei der Erhebung und Vernetzung von Informationen stoßen wir immer schnell an die datenschutzrechtlichen Notwendigkeiten, Bedingungen und Begrenzungen, die wir keineswegs bedenkenlos beiseite schieben dürfen. Sie sind ein wichtiger Teil unserer freiheitlichen Ordnung. Auf der anderen Seite müssen wir aber auch darauf achten, dass wir uns nicht in einem Maße von Informationen abschneiden, das uns dann am Ende unmöglich macht, richtige Antworten auf neue Herausforderungen zu finden.

[...]

Anlage 6

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
am 1. Oktober 2001

Sondertreffen der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z.B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

Anlage 7

Bundesministerium des Innern: Fragen und Antworten zum ePass allgemein

Woran ist ein ePass erkennbar?

Das Symbol auf dem Umschlag des elektronischen Passes steht für den ePass.

Der ePass-Chip befindet sich in der Passdecke und ist mit bloßem Auge nicht erkennbar.

Welche Daten sind im ePass gespeichert?

Im ePass-Chip sind personen- und dokumentenbezogene Daten gespeichert:

- zur Person: Vor- und Nachname, Geburtsdatum, Geschlecht, Staatsangehörigkeit;
- zum Dokument: Seriennummer, ausstellender Staat, Dokumententyp und Gültigkeitsdatum.

Außerdem sind im ePass sogenannte biometrische Daten gespeichert:

- im ePass der ersten Generation (Antragsdatum bis 31. Oktober 2007) das Passfoto;
- im ePass der zweiten Generation (Antragsdatum ab 1. November 2007) das Foto und zwei Fingerabdrücke.

Anlage 8

Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen

Stand Juli 2003

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel
Dr. Claudia Golembiewski, Dr. Thomas Probst

[...]

2.1 Überblick über den Stand des Einsatzes biometrischer Verfahren

Der Begriff *Biometrie* stammt aus dem Griechischen und leitet sich aus den griechischen Worten *bios* (= Leben) und *metrein* (= messen) her. Er wird im Zusammenhang mit der zahlenmäßigen Beschreibung und Vermessung im Bereich der Biologie, insbesondere der medizinischen Statistik, verwendet. Erst seit kürzerer Zeit wird er häufiger mit der automatischen Vermessung des menschlichen Körpers und einer damit möglichen automatisierten (Wieder-) Erkennung in Verbindung gebracht.[1]

[...]

Anlage 9

Flughafen Frankfurt 2007: Fracht und Passage mit neuen Spitzenwerten
15.01.2008

Konzernweit mehr als 75 Millionen Fluggäste – Dezember setzt Rekordserie in Frankfurt fort

Im zurückliegenden Jahr wurde am Frankfurter Flughafen erstmals die Rekordzahl von 54 Millionen Passagieren übertroffen. Gleichzeitig erreichte der Frachtumschlag am internationalen Drehkreuz FRA innerhalb eines Jahres zum ersten Mal die Marke von 2,1 Millionen Tonnen. Insgesamt zählte der Frankfurter Flughafen 54.167.817 Fluggäste – gegenüber dem Vorjahreswert eine Steigerung um 2,5 Prozent. Beim Frachtumschlag erzielte der Frankfurter Airport ein Plus von 1,9 Prozent auf 2.095.293 Tonnen.

[...]

Anlage 10

[...]

SICHERHEIT IST UNSER KERNGESCHÄFT

Unsere ID-Dokumente zählen zu den sichersten der Welt

In zahlreichen nationalen und internationalen Projekten haben wir dazu beigetragen, dass sich Menschen rund um den Globus sicher und frei bewegen können. Unsere ID-Dokumente zählen zu den sichersten der Welt. Technologisch setzen unsere Produkte und Lösungen innovative Maßstäbe. Und in der Entwicklung hochsicherer ID-Systeme gehören wir zu den wenigen global anbietenden Unternehmen, die nicht nur den Anspruch, sondern auch die Erfahrung haben, um ganzheitlich konzipierte Sicherheitsstrategien über die gesamte ID-Prozesskette kompetent und verlässlich steuern zu können.

Identität ist mit allen Mitteln zu schützen

Ein wesentlicher Motor unseres Erfolges ist das frühzeitige Erkennen und Aufgreifen veränderter Sicherheitsanforderungen. Mit dem Aufbau des ersten deutschen Trustcenters haben wir auf die wachsende Bedeutung von Public-Key-Infrastrukturen (PKI) und elektronischen Signaturen reagiert. Mit der Entwicklung des EU-Kartenführerscheins konnten wir hinsichtlich der eingesetzten Sicherheitsmerkmale und Materialien weltweit neue Standards definieren. Und mit der Generalunternehmerschaft im initialen Einführungsprozess des europäischen ePasses in Deutschland ist es uns gelungen, neueste Verfahren zur Sicherung und Weiterverarbeitung biometrischer Daten im gesamten ID-Prozess abzubilden und umzusetzen.

Identität ist eines der wichtigsten Güter, das wir Menschen besitzen. Um sie mit allen zur Verfügung stehenden Mitteln abzusichern, gilt es immer wieder, technologische Grenzen zu überwinden und neue Zukunftsoptionen zu eröffnen.

Borders are there to be crossed – Dafür setzen wir uns ein.

[...]

Anlage 11

EUROPÄISCHES PARLAMENT

2004 2009

Plenarsitzungsdokument

ENDGÜLTIG
A6-0174/2005

31.5.2005

*

BERICHT

über die Initiative der Französischen Republik, Irlands, des Königreichs Schweden und des Vereinigten Königreichs für einen Rahmenbeschluss des Rates über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus
(8958/2004 – C6-0198/2004 – 2004/0813(CNS))

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

Berichterstatter: Alexander Nuno Alvaro

[...]

Der Berichterstatter geht jedoch davon aus, dass es sich bei den vorgeschlagenen Maßnahmen um zwei getrennte Bereiche handelt. Zum einen soll im vorliegenden Ratsvorschlag unter anderem die Verpflichtung zur Aufbewahrung der Daten durch die *Service Provider*, die Definition der Daten und die Dauer der Aufbewahrung festgelegt werden, was in den Bereich des Gemeinschaftsrechts fällt. Zum anderen geht es neben anderem um den Zugang und den Austausch der gespeicherten Daten innerhalb der Mitgliedstaaten, wobei es sich um ein gemeinsames Vorgehen im Bereich der justiziellen Zusammenarbeit in Strafsachen handelt, der somit in den Bereich des dritten Pfeilers fällt.

Bereits heute existieren Gemeinschaftsregelungen bzgl. der Verpflichtung von *Service Providern*. Bei den hier in Frage stehenden Daten handelt es sich um Daten i. S. d. Art. 1 i. V. m. Art. 2 a der Richtlinie 95/46/EG vom 24. Oktober 1995. Die Richtlinie behandelt die allgemeinen Verpflichtungen der Mitgliedstaaten zur Gewährleistung des Schutzes der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten. Des weiteren wird durch die Richtlinie 2002/58/EG vom 12. Juli 2002 speziell die Verarbeitung personenbezogener Daten und der Schutz der Privatsphäre in der elektronischen Kommunikation geregelt. Das hinter beiden Regelungen stehende Prinzip besagt, dass die gespeicherten Daten dann zu löschen sind, wenn ihre Aufbewahrung sich nicht mehr rechtfertigt. Die Möglichkeit der Aufbewahrung von Daten wird den einzelnen Mitgliedstaaten ausnahmsweise in Art. 15 der Richtlinie 2002/58/EG eröffnet, sofern es zur Bekämpfung der Kriminalität notwendig, angemessen und verhältnismäßig erscheint. Auf eine Aufbewahrungsfrist konnten sich die Mitgliedstaaten in den Verhandlungen zur Datenschutzrichtlinie für Kommunikation nicht einigen und es wurde auf eine Festlegung verzichtet.

Damit steht die vom Rat gewählte Rechtsgrundlage der Bestimmung des Art. 47 EUV entgegen, wonach der EUV die Vorschriften des Vertrages zur Gründung der Europäischen Gemeinschaft (EGV) unberührt lässt. Demnach darf keine Regelung des EUV sich auf die Bestimmungen des EGV auswirken. Die Auswirkung auf das Gemeinschaftsrecht ergibt sich im vorliegenden Fall aus der Nichtbeachtung des bereits existierenden gemeinschaftlichen Rechtsrahmens. Daher fällt unter anderem die Verpflichtung der Provider zur Speicherung an sich, die Definition der zu speichernden Daten sowie die Aufbewahrungsdauer in den Regelungsbereich des EGV.

Die hier vorgeschlagenen Maßnahmen müssen aus logischen Gründen auf derselben Rechtsgrundlage basieren wie der bereits bestehende Rechtsrahmen. Damit wäre auch hier Art. 95 EGV zugrunde zu legen, der das Verfahren der Mitentscheidung vorsieht.

Diese Auffassung wird durch den Rechtsausschuss des Europäischen Parlaments gestützt. Der Berichterstatter wurde darüber informiert, dass sowohl der juristische Dienst der Europäischen Kommission als auch der des Rates mit dieser Rechtsauslegung übereinstimmen.

2. Verhältnismäßigkeit der Maßnahme

Darüber hinaus bezweifelt der Berichterstatter die Verhältnismäßigkeit der Maßnahmen im Einzelnen. Sie stehen nicht in einer angemessenen Zweck-Mittel-Relation, da sie weder geeignet noch erforderlich sind und eine unzumutbare Härte für die Betroffenen darstellen.

Bei dem zu speichernden Datenvolumen insbesondere im Bereich des Internets bezweifelt der Berichterstatter, dass eine zielführende Auswertung der Daten überhaupt möglich ist.

Teilnehmer aus dem Umfeld der organisierten Kriminalität und des Terrorismus werden die Verfolgbarkeit ihrer Daten leicht zu verhindern wissen. Möglichkeiten hierzu wären der Erwerb von Telefonkarten durch Strohmänner oder wechselnd eingesetzte Mobiltelefone von ausländischen Anbietern, die Nutzung öffentlicher Telefonzellen, die Veränderung der bei der Nutzung eines E-Mail-Service verwendeten IP-Adresse oder E-Mail-Adresse oder gleich die Nutzung von Internet *Service Providern*, die außerhalb Europas liegen und einer Verpflichtung bezüglich der Vorratsdatenspeicherung nicht unterliegen.

Sofern sämtliche von dem Vorschlag umfasste Verkehrsdaten tatsächlich gespeichert werden müssten, würde im Netz eines großen Internet-Providers bereits bei heutigem Verkehrsaufkommen eine Datenmenge von 20 - 40.000 Terabyte anfallen. Dies ist ein Datenvolumen, das ungefähr 4 Mio. km gefüllter Aktenordner entspricht - dies entspricht wiederum zehn Aktenbergen, die jeweils von der Erde bis zum Mond reichen würden. Bei dieser gewaltigen Datenmenge würde ein einmaliger Suchlauf bei einem Einsatz der vorhandenen Technik ohne zusätzliche Investitionen 50-100 Jahre dauern. Die rasche Verfügbarkeit der angeforderten Daten ist somit zu bezweifeln.

Gegenüber dem bestehenden Vorschlag der umfassenden Vorratsdatenspeicherung könnte das Mittel der anlassbezogenen Speicherung, welches u. a. auch von der *Cybercrime-Convention* des Europarats[1] vorgegeben ist, sowohl gleich geeignet als auch milder sein.

Mit Blick auf die Begründung des Rates zur Ablehnung dieser Alternative[2] drängt sich die Frage auf, inwiefern die vorgesehene Vorratsdatenspeicherung mit dem Prinzip der Unschuldsvermutung vereinbar ist.

Der vorliegende Vorschlag geht außerdem nicht auf die möglichen Belastungen der Betroffenen ein. Neben den tiefen Eingriffen in den Schutz der persönlichen Daten des Einzelnen, sind enorme Belastungen für die europäische Telekommunikationsindustrie, insbesondere für kleinere und mittlere Telekommunikationsunternehmen zu befürchten.

Kosten erwachsen in diesem Zusammenhang vor allen Dingen aus:

- der Anpassung der Systemtechnik zur Generierung und Speicherung der Daten,
- der Anpassung der betrieblichen Abläufe zur sicheren Archivierung der Daten sowie
- der Bearbeitung und Auswertung von Anfragen der Sicherheitsbehörden.

Der hierfür erforderliche Investitionsaufwand im Bereich der klassischen leitungsvermittelten Telefonie liegt nach Schätzungen verschiedenster größerer Unternehmen innerhalb der

[1] ETS Nr. 185, 8. November 2001; die Konvention wurde noch nicht in allen Mitgliedstaaten umgesetzt.
[2] Ratsdokument 8958/04 ADD 1. In dem erläuternden Dokument zum Rahmenbeschluss über die Vorratsdatenspeicherung wird lediglich festgestellt, dass die anlassbezogene Speicherung von Daten "keinen Beitrag zur Überprüfung von Personen leisten kann, die noch nicht verdächtigt werden, einer kriminellen oder terroristischen Organisation anzugehören [...] Sie kann daher nicht den Bedarf der Sicherheits-, Geheimdienst- und Strafverfolgungsstellen im Hinblick auf die Bekämpfung heutiger Straftäter, zu denen auch Terroristen gehören, decken"

[...]

Anlage 12

Di 15. Mai 07

Veröffentlichung des Verfassungsschutzberichts 2006

Rede von Bundesminister Dr. Wolfgang Schäuble anlässlich der Vorstellung des Verfassungsschutzberichts 2006 am 15. Mai 2007 in Berlin

[...]

Es ist eine der entscheidenden Zukunftsaufgaben, die Kooperation zwischen unseren Sicherheitsbehörden bei der Gefahrenabwehr zu optimieren. Prävention wird nur dann dauerhaft erfolgreich sein, wenn wir das Netz zwischen den Behörden möglichst engmaschig knüpfen. So müssen die Vorfeldaufklärung des Verfassungsschutzes und die dort gesammelten Erkenntnisse – natürlich unter Beachtung rechtsstaatlicher Grundsätze – mit den polizeilichen Gefahrabwehrmöglichkeiten in Beziehung gesetzt werden.

Das gilt gerade auch bei der Beobachtung des Internets. Terroristische Aktivitäten verlagern sich immer mehr in die virtuelle Welt des world wide web. Das Internet bietet den Terroristen ein gigantisches Forum: Es ist Kommunikationsplattform, Werbeträger, Fernuniversität, Trainingscamp und think tank in einem.

Deshalb brauchen wir im nachrichtendienstlichen Bereich die Möglichkeit der so genannten Online-Durchsuchung. Denn wir können nicht die Augen vor der technischen Entwicklung verschließen. Auf selbst verordnete Blindheit nehmen Terroristen keine Rücksicht. Natürlich müssen wir eine derart sensible Materie sorgsam und abgewogen angehen, wir brauchen eine verfassungsrechtlich einwandfreie, sichere und klare Rechtsgrundlage. Diese werden wir schaffen – falls erforderlich auch durch eine Ergänzung des Grundgesetzes.

[...]

ERKLÄRUNG:

„Ich versichere, dass ich diese Diplomarbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe."

Aspach, den 25. Februar 2008